IRREGULAR WARFARE CENTER
INSIGHTS
Vol. 3, No. 2, July 2025

Blueprint to Counter China's Criminal State Actions: *Leveling the Playing Field for Strategic Competition*

BLUF: The People's Republic of China (PRC) is leveraging rogue, unconventional espionage to target U.S. civilian companies and critical infrastructure. By straying from the international norms surrounding espionage, the PRC has gained asymmetric strategic advantage that must be countered. To do so, the United States needs to engage in international action to create a comprehensive response across the range of U.S. and foreign apparatus needed to establish a level playing field in the global arena.

As athletes from around the globe vied for medals in Paris, the 2024 Olympic Games also highlighted the importance of upholding international standards. On 7 August 2024, the Olympic Committee hosted a long-awaited medal ceremony for the 2022 Figure Skating Team Event, which the committee originally postponed due to a doping scandal involving a Russian athlete. After a thorough investigation revealed that the athlete had tested positive for banned substances, the Russian team was disqualified. Consequently, the gold and silver medals were awarded to the United States and Japan, respectively, marking a pivotal moment in the ongoing commitment to fair competition.

Just as the Olympic Charter governs sports, nation-to-nation competition should adhere to international norms. Yet, China's actions, from economic theft to malware attacks on critical infrastructure, violate the rules-based international order. By straying from the international norms

AUTHORS:
DR. JEFF GARDNER - *Chief of Faculty & Curriculum – Irregular Warfare Center*
VARSHA KODUVAYUR – *Senior Analyst – Irregular Warfare Center (Valens Global CTR)*
ELIZABETH TURNAGE – *Analyst – Irregular Warfare Center (Valens Global CTR)*

IWC MISSION: The IWC prepares the warfighter to conduct irregular warfare across the spectrum of conflict by bridging instruction to operationalizing IW using next-generation techniques and concepts that enhance the lethality of the force and positions the United States and key Allies and partners to remain ahead of the threat.

surrounding espionage, the PRC has gained asymmetric strategic advantage that must be countered. It is time for the United States and its allies to level the playing field against China.

PRC ESPIONAGE AND ITS THREAT TO U.S. NATIONAL SECURITY

The PRC employs whole of society espionage tactics that differ markedly from those commonly practiced in most nations. As a result, the PRC has enjoyed an asymmetric advantage that poses significant risk to both individual U.S. businesses and our strategic standing as a whole.

In simple terms, while most nations use government resources to spy on other governments, the PRC leverages everyday civilians and businesses to target U.S. civilian infrastructure. For example, the PRC's government-sponsored talent plans that recruit foreign nationals in industries of interest to enter into contracts with the PRC and steal technology that could benefit the state. One such program entitled Young Thousand Talents (YTT) recruits foreign STEM students to travel to China, where they conduct and publish research in areas related to the state's national security. Other examples of the PRC targeting civilians include bribing disgruntled employees with money and "women" to create insider threats, and employing aggressive cyber intrusions through hacking and phishing to gain access to intellectual property through the companies own computer networks.

Beijing has sought to target a broad array of strategic industries. As of October 2023, the FBI reported over 2,000 active investigations into PRC-related thefts spanning industries such as agriculture, biotech, healthcare, robotics, aviation, energy, critical infrastructure, and academic research. These thefts include the pilfering of intellectual property, trade secrets, and other sensitive data.

Beyond targeting industries, PRC intelligence agents are infiltrating and embedding malware into our critical infrastructure Supervisory Control and Data Acquisition (SCADA). SCADAs are systems that help monitor and control industrial processes remotely, like managing water treatment plants or power grids, by collecting real-time data from sensors and allowing operators to adjust settings and respond to issues. A prime example of such espionage on sensitive data is the PRC-sponsored cyber group Volt Typhoon, who use cyber espionage tactics to compromise critical energy, communications, transportation, and water infrastructure across the United States. As a result, the PRC have been able to position themselves for a potentially devastating cyber-attack impacting the lives of everyday Americans. The FBI also emphasized that these efforts are "unprecedented" and exceed the bounds of traditional Western espionage practices.

Consider, for example, Yanjun Xu, the first Chinese intelligence agent to be extradited to the United States and convicted for economic espionage and conspiracy to commit trade secret theft. According to the Department of Justice (DoJ), Xu became a member the Chinese Ministry of State Security (MSS) in 2003. By 2013, Xu was targeting U.S. aviation companies to steal proprietary technology for the benefit of the Chinese state.

Xu's scheme recruiting American employees to travel to China and using front companies and universities to deceive them. Once deceived, MSS operatives hacked into the computers of aviation employees to gain access to proprietary data. For example, in 2017 Xu solicited a General Electric (GE) Aviation employee to give a presentation at a Chinese university, and later requested "system specification [and] design process" details on proprietary information.

In addition to his own attempts at economic espionage, Xu directed other Chinese spies to conduct acts of espionage. For example, Xu provided Chinese national Ji Chaoqun, then a student in Chicago,

with names of American individuals to collect information on for the purposes of potentially recruiting them to work for the PRC.

The Xu scheme was quite large. According to the DoJ, the scheme included a number of Chinese nationals who worked in a variety of companies—including U.S. defense contractors—across the United States in an attempt to gain access to aerospace and satellite technology.

The Xu story serves to show the diversity of the PRC's espionage tactics. He targeted industry employees, "buttered them up" through trips to China, and employed cyber espionage techniques to gain access to proprietary data. It also exemplifies the scale of PRC espionage—illuminating the tip of the iceberg of potential networks of PRC actors across the United States. While Xu's capture marked an end to one scheme, PRC espionage continues, with the United States sentencing yet another agent of the PRC collecting information on American individuals on 6 August 2024.

The Impact of PRC Espionage

The PRC's unconventional espionage scheme poses a significant threat to both U.S. companies and the country as a whole. Such theft allows Chinese companies to adopt technological advancements without the extensive research and development costs that western companies invest in them. The effects are twofold: PRC companies are no longer dependent on U.S. companies to supply the technology, and PRC companies are able to export stolen technology to sell abroad at a lower cost than the developer. Thus, the developer not only loses clients, but can also be priced out of the industry.

From a strategic level, damage to individual businesses could have widespread impacts on the United States. From an economic standpoint, intellectual theft allows the PRC to expedite industrial development, and may eventually—according to the FBI—allow China to "dominate key industries" in order for the state to "topple our status" in the global arena.

Furthermore, PRC access to our infrastructure SCADA could have outsized effects to the United States, with the PRC potentially possessing the power to disrupt water and electricity. As emphasized by the FBI , such power could be used to strategically "wreak havoc" in the United States, possibly acting as a deterrent or strategic response to an event of conflict. As such, PRC espionage potentially opens the door to a PRC invasion of Taiwan where the United States has little ability to respond.

CONFRONTING PRC ESPIONAGE: *GO TOGETHER, GO FAR*

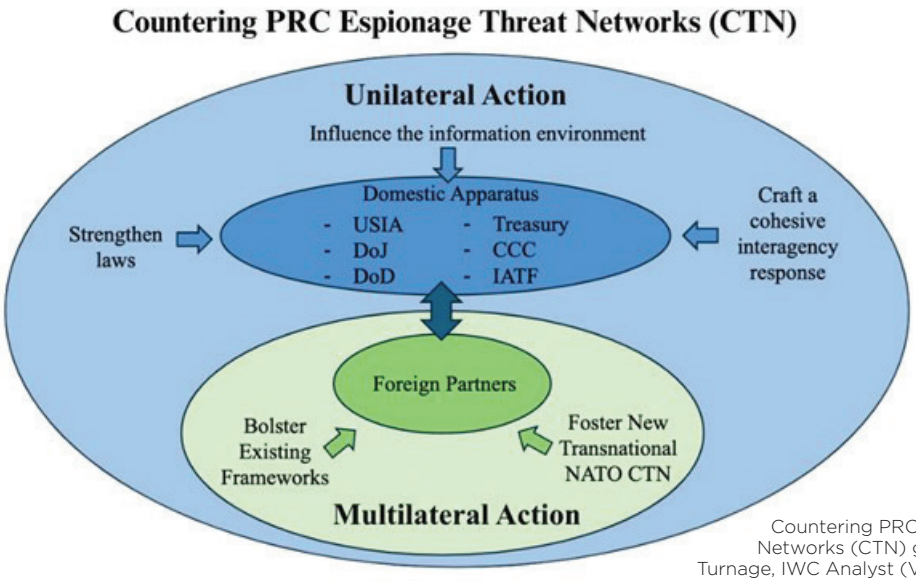
The United States should consider expanding existing international frameworks while creating new partnerships to increase U.S. and allied presence in the Indo-Pacific and create a comprehensive response to PRC espionage. This will counter the asymmetric advantages of PRC espionage and promote a level playing field among international actors.

The first option available for the United States on the global stage is to expand existing multilateral programs to build response capabilities in the Indo-Pacific. One opportunity to achieve this end is in NATO, where many lobby for the expansion of Article 5, which dictates the conditions of engagement for NATO members, to include Hawaii. As it stands, Article 5 states that the NATO treaty only protects territories north of the Tropic of Cancer—excluding the Hawaiian archipelago and other territories such as Puerto Rico, the Virgin Islands, French Guyana, the Falkland Islands, Guam, and American Samoa from formal protection under the treaty. Should the article be amended to include member territory below the tropic, the United States and our allies would establish a significant NATO presence in the Indo-Pacific to stand against the PRC.

An additional opportunity to expand existing agreements lies within the trilateral security partnership between Australia, the United Kingdom, and the United States (AUKUS). As it stands, AUKUS contains an initiative to "enhance joint capabilities and interoperability, focusing on cyber capabilities, artificial intelligence, quantum technologies and additional undersea capabilities." By increasing emphasis on cyber capabilities, this partnership could allow multilateral innovation and defense against rogue PRC espionage.

Finally, the United States should push allies to adopt a counter threat network (CTN) to create a comprehensive, organized approach to counter rogue PRC espionage that threatens the international community. Such a program would not only help the United States, but other allies who have similarly experienced asymmetric PRC espionage.

Given that U.S. allies are experiencing the same threat, these organizations should move to create a CTN to facilitate an effective counter to the PRC. As previous research has shown, CTNs require strong ties and productive cooperation between all sectors of government apparatus—including the military, intelligence community, financial sector, and law enforcement—to achieve success. A multilateral CTN could not only serve as a platform for information sharing, but also foster collaboration between members to enact countermeasures to the growing threat of PRC espionage. To fully achieve this goal, the multilateral CTN should work in close cooperation with domestic efforts to ensure that the diverse threats are comprehensively rebutted. As depicted by the figure below, the success of this international CTN is dependent on alignment with domestic efforts.



Countering PRC Espionage Threat Networks (CTN) graph by Elizabeth Turnage, IWC Analyst (Valens Global CTR)

Given its immense commercial and strategic impacts, rogue PRC espionage presents a critical threat to U.S. interests—and to those of our allies. These threats are complex and unconventional, with the PRC targeting a wide range of civilian and critical infrastructure nodes.

Strategic competition with the PRC should start with both domestic and multilateral action to counter these criminal activities and violations of international norms. The future of U.S. industry, security, and stability depends upon leveling the playing field against PRC espionage.