Testimony Before the U.S. House of Representatives Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party

Jill I. Goldenziel

September 19, 2024

Disclaimer: The views presented are those of the speaker and do not necessarily represent the views of the National Defense University, the U.S. Department of Defense, or its Components.

Chairman Moolenaar, Ranking Member Krishnamoorthi, and Members of the Committee: thank you for the invitation to testify as you consider the critical matter of how to counter the PRC's legal warfare.

I am a Professor at the National Defense University's College of Information and Cyberspace, where I write and teach about international and constitutional law, national security strategy, information warfare, and legal warfare. I am also a non-resident Fellow at NATO's Supreme Headquarters Allied Powers Europe/Allied Command Operations' Office of Legal Affairs and a Senior Affiliated Scholar at the University of Pennsylvania's Fox Leadership International Program. I am a columnist for *Forbes.com* and *Bloomberg Opinion*. Previously, I served as a Professor at Marine Corps University and a Lecturer at Harvard College and Harvard Law School. I regularly advise U.S. Combatant Commands, military forces, the intelligence community, other civilian agencies, and U.S. allies and partners on countering legal warfare by U.S. competitors and adversaries. Last week I was in the Philippines, teaching Philippine military lawyers about countering legal warfare and getting a firsthand look at the challenges that PRC legal warfare presents for U.S. forces and our allies and partners.

The People's Republic of China is weaponizing law in its strategic competition against the United States. Legal warfare is a fundamental pillar of the PRC's civil-military fusion strategy.[1] The PRC uses legal warfare to undermine the rules-based international order and to set the conditions to export authoritarianism and advance its military and strategic interests. Legal warfare thus poses a threat to U.S. national security. The PRC routinely passes domestic laws to lend a veneer of legitimacy to its behavior that does not comport with international law. The PRC is also exporting its authoritarian model to harass people within the United States, harming their Constitutional freedoms in the process.[2]

PRC State-Owned Enterprises (SOEs) and corporations are acting consistently with the PRC's legal warfare strategy. Some PRC-based entities may be using the PRC's domestic laws to

---

[1] Jill I. Goldenziel, *Law as a Battlefield: The U.S., China, and the Global Escalation of Lawfare*, 106 CORNELL L. REV. 1085, 1092-93 (2021).

[2] *See, e.g.*, Complaint, United States v. Xinjiang Jin, No. 20-MJ-1103 (E.D.N.Y. Dec. 18, 2020), available at https://www.justice.gov/usao-edny/press-release/file/1346966/dl; Complaint, United States v. Zhu Feng et al., No. 20-MJ-1025 (PK) (E.D.N.Y. Oct. 27, 2020); proceeding as United States v. Ji Hu et al., No. 1:21-CR-00265 (E.D.N.Y.) (adding an additional defendant).

stall litigation in U.S. courts.[3] Others are using the U.S. legal process to access national security-sensitive intellectual property.[4] Some of these actions may represent standard litigation tactics by businesses using the legal system to defend their interests. However, if these actions are systematically backed by the PRC itself as part of a legal warfare strategy, they represent an attempt to subvert and undermine the U.S. legal process and the rights of Americans. For example, PRC-based entities have filed multiple high-profile libel suits against individual researchers, nonprofits, and media outlets who criticize the PRC in U.S. courts and the courts of other democracies.[5] If the PRC is backing spurious lawsuits in U.S. courts as part of a legal warfare strategy, it would be a clear violation of Constitutional rights.

Congress must act to counter PRC legal warfare and its threat to the rules-based international order. Pending legislation in the Senate Draft of the Fiscal Year 2025 National Defense Authorization Act (NDAA) represents an important start, but countering PRC legal warfare requires a national-level strategy and a whole-of-government approach.[6] This testimony will proceed by providing a brief explanation of the PRC's overarching legal warfare strategy. I will then discuss attempts and possible attempts by the PRC and PRC-based entities to use legal warfare within the U.S. legal system, distinguishing between standard use of the U.S. legal system and possible legal warfare efforts backed by the PRC state. I will then discuss some considerations for Congress in addressing the threat of PRC legal warfare while protecting the civil liberties of U.S. persons.

I. Defining the Threat of Legal Warfare

Legal warfare, often translated as "lawfare," is essential to the PRC's political and military efforts. Legal warfare is one of "The Three Warfares" that underpin the PRC's civil-military fusion strategy, together with public opinion warfare and media warfare.[7] The PRC uses the Three Warfares in tandem, inside and outside of armed conflict, as part of its political warfare efforts. The Three Warfares shape perceptions favorable to the PRC and unfavorable to its competitors and adversaries, while hindering its adversaries' capacity to respond.[43]

No authoritative doctrinal definition of legal warfare exists in U.S. or PRC military or government publications. The U.S. Indo-Pacific Command and U.S. European Command have adopted a definition I developed in a 2021 *Cornell Law Review* article in their Counter-Lawfare Programs, which were developed to counter legal warfare by the PRC and other adversaries. I

---

[3] *See* Kirk J. Nahra, Lester Ross, and Allison Binxue Que, *Navigating China's Data Security Laws in US Discovery*, WILMERHALE CLIENT BULLETIN, April 3, 2024.

[4] Representative filings include Soaring Wind Energy v. CATIC USA Inc., 946 F.3d 742 (5th Cir. 2020); AVIC Int'l Holding Corp. v. Soaring Wind Energy, 946 F.3d 742 (5th Cir. 2020), *cert. denied*, 131 S.Ct. 619 (Oct. 19, 2020) (Nos. 20-39 & 40); In re AVIC International USA Inc., No. 2:20-19043; KLEO AG v. Rivada Networks, Inc., No. 22-cv-01664 (DLF), 2023 WL 7921969 (D.D.C 2023), *appeal docketed*, No. 23-7175 (D.C. Cir. 2023). A full list of cases in the Tang/AVIC and KLEO Rivada matters is too numerous to cite here, and the terms of the Tang/AVIC settlement are confidential.

[5] *See infra* notes 24-30.

[6] U.S. Senate Armed Services Committee, National Defense Authorization Act for Fiscal Year 2025 (Bill), § 1284, 118th Cong., (2024), available at https://www.armed-services.senate.gov/imo/media/doc/fy25_ndaa_executive_summary.pdf

[7] Goldenziel, *Law as a Battlefield*, *supra* note 1, at 1092.

defined "lawfare" as the purposeful use of law "1) taken toward a particular adversary with the goal of achieving a particular strategic, operational, or tactical objective, or 2) to bolster the legitimacy of one's own strategic, operational, or tactical objectives toward a particular adversary, or to weaken the legitimacy of a particular adversary's strategic, operational, or tactical objectives."[8]

PRC legal warfare, however, goes beyond this basic definition. PRC legal warfare aims to distort international law and subvert the rules-based international order and the U.S. Constitutional order. The PRC employs legal warfare with the goal of factionalizing its adversaries and weakening their will to fight. Legal warfare shapes the legal context and international and domestic narratives to support the PRC's geopolitical aims. The PRC views legal warfare as a form of combat in its own right. Chinese authors give equal importance to preparing the legal and physical battlefields for competition and combat and emphasize strong coordination between legal and kinetic warfare. The PRC views legal warfare as a way to portray its aggressive and authoritarian acts as legitimate, enabling it to seize the initiative and to weaken international resistance to their political and military actions. Seizing legal standards and using them flexibly is a key principle underpinning legal warfare. The PRC aims to gain "legal principle superiority" over its adversaries to ultimately control the meaning of international law itself.

The PRC is using legal warfare to legitimize its illegal maritime claims in the South and East China Seas. In his testimony before Congress this Spring, the Commander of the U.S. Indo-Pacific Command recognized this legal warfare as a threat to U.S. interests.[9] For example, the PRC is using maritime militia vessels, driven by civilian fishermen who work part-time on the People's Liberation Army's payroll, to illegally threaten the Philippines' rights in its exclusive economic zone and to support Chinese Coast Guard efforts to water cannon, laser, and ram Philippine vessels. The maritime militia attempts to legitimize PRC presence in the Japan-administered Senkaku Islands while eroding principles of the law of armed conflict and complicating any response by law-abiding nations. By using civilian vessels for a military purpose to conduct gray zone operations, the PRC erodes the principle of distinction at the core of the law of armed conflict. The PRC also routinely creates new domestic laws and institutions to justify enforcement of their domestic claims. For example, its Coast Guard Law authorizes the PRC Coast Guard to conduct illegal activities in its neighbors' EEZs and to detain foreign personnel in maritime zones that the PRC illegally claims as its own.[10]

Applied in U.S. courts, PRC legal warfare is distinct from standard use of the U.S. legal system by foreign companies. Standard users of a legal system work within the system and respect the rule of law. PRC legal warfare aims to undermine democratic legal systems and international law and reshape the rules-based order in its favor. Standard users of a legal system seek to advance their interests while playing by the rules. PRC legal warfare ultimately seeks to rewrite the rules, change the game, and control the league.

---

[8] Goldenziel, Law as a Battlefield, *supra* note 1, at 1097.

[9] *U.S. Indo-Pacific Command Posture: Hearing Before the H. Armed Servs. Comm.*, 108th Cong. 9 (2024), available at https://www.congress.gov/118/meeting/house/116960/witnesses/HHRG-118-AS00-Wstate-AquilinoJ-20240320.pdf

[10] Jill Goldenziel, *China's New Coast Guard Law Means More Maritime Mayhem*, FORBES (July 31, 2024), available at https://www.forbes.com/sites/jillgoldenziel/2024/07/31/chinas-new-coast-guard-law-means-more-maritime-mayhem/

II. How the Legal Great Wall Increases Risks for U.S. Businesses and Individuals

The PRC's self-styled "Legal Great Wall" has changed the parameters of doing business in the PRC and poses a risk to U.S. individuals and firms doing business in the PRC or with PRC-based entities. The PRC has built what it calls a "Legal Great Wall," more than 20 laws passed in recent years ostensibly to safeguard its national security.[11] In 2023, the National Counterintelligence and Security Center of the Office of the Director of National Intelligence published a list of eight national security, cyber security, and data protection laws passed or updated by the PRC since 2015 that pose risks to U.S. businesses in the PRC and U.S. firms and individuals doing business with PRC entities.[12] Individually and together, the laws expand the PRC's oversight of domestic and foreign companies operating within the PRC and extend PRC control over those companies' data, including to data outside the PRC. The PRC has also applied its data protection laws against individuals and firms in the United States to silence critics and infringe on their Constitutional rights. PRC-based litigants may also be using these laws to delay proceedings in U.S. courts.

2023 updates to the PRC's National Security Law and Anti-Espionage Law are of particular concern for U.S. national security and business interests. While all countries take measures to protect national security and counter spying, these laws tighten the PRC's authoritarian control over all entities doing business in the PRC or with PRC-based entities. The National Security Law outlines whole-of-society responsibilities for the PRC's national security aims. Under the law, all PRC citizens and private organizations must assist the PRC government and intelligence services with undefined national security matters whenever ordered. The law may be used to compel PRC nationals employed by U.S. firms in the PRC to assist in investigations against U.S. corporations and individuals.

Perhaps even more concerning for U.S. businesses is the Anti-Espionage Law.[13] Before 2023, the law only covered state secrets and intelligence. The 2023 update expanded the PRC's definition of espionage to cover "all documents, data, materials concerning to national security and interests included for protection." The terms "national security" and "interests" are not defined. The law defines espionage as "collaborating with spy organizations and their agents," and espionage activities "conducting cyber-attacks against state entities, confidential-related units, or

---

[11] Xinhua News Agency, *China builds Legal Great Wall to Safeguard National Security: Official*, CHINA DAILY, Apr. 25, 2024, available at https://global.chinadaily.com.cn/a/202204/25/WS62663de4a310fd2b29e5926d.html

[12] Nat'l Counterintelligence & Sec. Ctr., *U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies*, SAFEGUARDING OUR FUTURE, (June 30, 2023) (describing China's 2023 Counter-Espionage Law, 2021 Personal Information Protection Law, 2021 Cyber Vulnerability Reporting Law, and 2021 Anti-Foreign Sanctions Law, 2021 Data Security Law, 2017 Cybersecurity Law, 2017 National Intelligence Law, and 2015 National Security Law), available at https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf. For discussion of 2024 revisions to the PRC's Law on Guarding State Secrets, *see* Lester Ross, *China Revised the State Secrets Law*, WILMERHALE CLIENT ALERT, March 1, 2024, available at https://www.wilmerhale.com/insights/client-alerts/20240301-china-revised-the-state-secrets-law

[13] China Law Translate, *Counter-Espionage Law of the PRC* (2023 ed.), available at https://www.chinalawtranslate.com/en/counter-espionage-law-2023/. *See also* Jill Goldenziel, *China's Anti-Espionage Law Raises Foreign Business Risk*, FORBES (July 3, 2024), available at https://www.forbes.com/sites/jillgoldenziel/2023/07/03/chinas-anti-espionage-law-raises-foreign-business-risk/

critical information infrastructure." "Joining espionage organizations and agents" is a category of espionage activity, but "joining" is not defined. "Inciting," "enticing," bribing," or coercing a foreign official to defect are also considered espionage activities. Analysts have expressed concern that the PRC may apply the law to regular business activities, such as business intelligence activities, market research, and hiring former government officials. Researchers and journalists could easily be accused of espionage for routine professional activities. Corporate users of data centers and cloud services in the PRC could be investigated if their data relates to national security. The PRC now has unprecedented powers to investigate individuals' electronic devices and inspect their business premises—and to collect sensitive data. Corporate officials may also be subject to exit bans while under investigation.

The PRC's laws related to data security pose additional risk for U.S. businesses, especially those who become litigants in U.S. courts. The 2021 Personal Information Protection Law (PIPL) authorizes the PRC to collect personal data for actions "in the public interest," requires domestic and foreign companies to comply with privacy reviews, controls handling of personal data within and outside mainland PRC when providing products or services to persons within the PRC and restricts the ability of companies operating in the PRC to collect and retain personal data. It also authorizes the PRC to collect personal data for any actions it deems to be in the public interest. The 2021 Data Security Law subjects cross-border data flows to new regulatory requirements and prohibitions and positions the PRC to control or deny cross-border data transfers, including from foreign governments. These two laws, along with the PRC's Cybersecurity Law, include broad categories of information and many ambiguities open to interpretation by both the PRC government and U.S. and PRC courts. PRC courts, interpreting these laws, have been generally reluctant to order data production in foreign judicial proceedings.[14]

PRC-based parties have used these laws to attempt to shield themselves from discovery in U.S. courts. For example, *Cadence Design Systems, Inc. v. Syntronic AB et al*. is one of the first significant decisions involving a discovery dispute in which PRC companies claimed that the Great Firewall prevents them from complying with discovery obligations in U.S. courts.[15] During discovery in the patent dispute, the plaintiff requested that the Beijing-based defendant produce computers located within the PRC. The defendant claimed PRC data laws, specifically the Personal Information Protection Law, barred production of the computers because the computers contained personal information, and consent of the relevant individuals was required to transfer the computers outside the PRC. Instead, Syntronic Beijing offered to allow the plaintiffs to review the computers in the PRC. The federal District Court for the Northern District of California held in favor of the plaintiffs, finding that the Personal Information Protection Law provides for an exception to the consent requirement if a request is made pursuant to a "foreign legal obligation." The Court interpreted this exception to include discovery requests in U.S. legal proceedings. A second U.S. court reached a similar interpretation in 2023.[16] This interpretation may be controversial in other cases.[17] It also remains to be seen whether PRC parties will comply with

[14] *See* Kirk J. Nahra, Lester Ross, and Allison Binxue Que, *Navigating China's Data Security Laws in US Discovery*, WILMERHALE CLIENT BULLETIN, April 3, 2024.
[15] Cadence Design Systems, Inc., v. Syntronic AB et al., 2022 WL 1320629, 21-cv-03610-SI, May 3, 2022.
[16] Owen and Wandling v. Elastos Foundation et. al, 2020 WL 6867754, 19-cv-5462, S.D.N.Y., Oct. 14, 2020.
[17] *See* Nahra, Ross, and Que, *supra* note 14.

U.S. court orders for production, or if they will face repercussions from the PRC government for doing so.

In many legal cases, invoking data protection laws to shield a client from discovery requests may simply be the prerogative of an attorney representing a PRC-based litigant in a U.S. court. However, PRC-backed entities' use of the Great Firewall as a shield to delay U.S. legal proceedings must be considered in the context of the PRC's overall legal warfare strategy. The PRC has consistently shown disdain for efforts to undermine dispute resolution proceedings in foreign and international courts, most famously its rejection of the 2016 South China Sea arbitration invalidating its illegal maritime claims in the South China Sea and a concurrent cyber-attack on the Permanent Court of Arbitration that has been attributed to PRC-based hackers.[18] Malware was implanted on the Permanent Court of Arbitration website while the dispute was in progress, infecting the computers of visitors, potentially exposing them to data theft. When the 2019 National Defense Authorization Act banned the U.S. government from using Huawei equipment, Huawei responded by filing a lawsuit against the U.S. that few believed they could win—and simultaneously hiring two U.S. public relations firms who promptly registered under the Foreign Agents Registration Act.[19] Huawei wished to publicize its claims that the ban violated due process and other Constitutional rights. Given this context, more research is needed to understand whether PRC-based parties are speciously using the Great Firewall as a tool to hinder discovery processes, and whether PRC courts or the CCP are systematically supporting them to do so as part of a legal warfare strategy.

The PRC is using the Legal Great Wall to assert control and export its authoritarian model. Risks for U.S. businesses and individuals have undoubtedly increased as the Legal Great Wall has grown higher. The PRC's crackdowns against foreign corporations and detention of their employees are increasing. A 2022 study by researchers at California Polytechnic State University found that at least 41 foreign businesspeople were subjected to exit bans in the PRC due to civil business disputes between 1995 and 2019, a number that the researchers say is a significant underestimation due to data limitations.[20] Recent reports suggest the numbers are rising. High-profile detentions of Canadian business travelers in 2018 also occurred in retaliation for the arrest of Huawei executive Sabrina Meng for violating U.S. law.[21] In this alarming context, the U.S. State Department updated its travel advisory for the PRC in 2023, citing the "risk of wrongful detentions" and "arbitrary enforcement of local laws."[22] The State Department also warns that attorneys are not permitted to take depositions in the PRC for use in foreign courts except through requests to its Central Authority, and that doing so could result in the arrest, detention, or

---

[18] China Sea Arbitration (Phil. v. China), Case No. 2013-19, Award, ¶ _765 (Perm. Ct. Arb. 2016).; Alliance for Securing Democracy, *China State-Affiliated Hackers Attack Permanent Court of Arbitration*, available at https://securingdemocracy.gmfus.org/incident/chinese-state-affiliated-hackers-attack-permanent-court-of-arbitration/

[19] Goldenziel, Law as a Battlefield, supra note 1, at 1130-34.

[20] Chris Carr and Jack Wroldsen, *Exit Bans When Doing Business in China*, 64 THUNDERBIRD INT'L BUS. REV. (2022) at 209-220; James Pomfret and Angel Woo, *China's Exit Bans Multiply as Political Control Tightens Under Xi*, REUTERS, May 1, 2023, available at https://www.reuters.com/world/china/chinas-exit-bans-multiply-political-control-tightens-under-xi-2023-05-02/

[21] Jill Goldenziel, *China's Legal Warfare Puts Business Executives at Risk,* FORBES (Aug. 13, 2021), https://www.forbes.com/sites/jillgoldenziel/2021/08/13/chinas-legal-warfare-puts-business-executives-at-risk/

[22] U.S. Dep't of State, *China Travel Advisory* (last updated July 18, 2023), available at https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories/china-travel-advisory.html

deportation of U.S. attorneys and deposition participants.[23] The Legal Great Wall thus extends the PRC's authoritarian reach to the data of U.S. businesses and individuals operating outside the PRC, and into U.S. legal proceedings.

III. How the PRC Exports Its Authoritarian Model to Target People Within the U.S.

The PRC does not hesitate to export its authoritarian reach to people within the United States and to undermine U.S. Constitutional rights and freedoms. In one egregious example, federal prosecutors charged a former Zoom executive in 2020 for disrupting and censoring video meetings involving U.S.-based participants that commemorated the Tiananmen Square massacre. Xinjiang "Julien" Jin, who is based in the PRC, allegedly fabricated reasons to suspend the Zoom accounts of individuals in New York who were hosting memorials and coordinated with PRC officials to identify meetings to target. He allegedly then logged into the video meetings using aliases and profile photos related to terrorism or child pornography. He then reported the meetings for violating Zoom's terms of service. Jin's actions resulted in the termination of at least four meetings, which were largely attended by U.S.-based users. Jin also allegedly shared the users' data with PRC authorities. The case represents a flagrant use of the PRC exporting its authoritarian model to suppress the First Amendment rights of persons based in the United States. Commenting on the case, FBI director Christopher Wray stated that "Americans should understand that the Chinese government will not hesitate to exploit companies operating in the PRC to further their international agenda, including repression of free speech."

The PRC has also sought to chill the free speech rights of its dissidents and fugitives living in the United States. In 2020, the Justice Department charged eight people with conspiracy in an extensive campaign to harass Chinese political dissidents and fugitives living in the United States on the PRC's behalf. "Operation Fox Hunt" employed private investigators, stalking, surveillance, and threats to the victims and their family members, aimed at pressuring them to return home to face trial.[24] The PRC's brazen attempts to harass these individuals on U.S. soil indicate its disregard for U.S. law.

Consistent with these actions by the PRC state, PRC entities are also filing lawsuits to silence and harass critics of the PRC in the United States and other democratic countries. These lawsuits bear the hallmarks of Strategic Lawsuits Against Public Participation, known as "SLAPP" suits. SLAPP suits typically bring frivolous defamation or libel claims against critics of a plaintiff's activities. SLAPP suits are intended to silence critics, drain their financial resources, and chill the free speech of others who might wish to speak out. More clearly problematic are lawsuits by PRC companies against individual media, journalists, and nonprofits who criticize the PRC or work against its interests. These lawsuits typically allege libel and defamation when critics point out the companies' state ownership or close ties to the PRC state. The goal of the suits is not necessarily to win; accordingly, some of these suits have been withdrawn after lengthy legal battles.

---

[23] U.S. Dep't of State, *China Judicial Assistance Country Information* (last updated Mar. 31, 2023), https://travel.state.gov/content/travel/en/legal/Judicial-Assistance-Country-Information/China.html

[24] United States v. Zhu Feng et al., No. 20-MJ-1025 (PK) (E.D.N.Y. Oct. 27, 2020) (complaint) (charged under 18 U.S.C. § 371), proceeding as United States v. Ji Hu et al., No. 1:21-CR-00265 (E.D.N.Y.) (additional defendant added).

In one prominent example, PRC electric vehicle behemoth BYD sued the non-profit Alliance for American Manufacturing and several of its employees in U.S. federal court.[25] AAM, formed in 2007 as a partnership between U.S. manufacturers and United Steelworkers, had argued that federal transit funds should not go to entities of concern or companies headquartered in non-market economies, including the PRC. AAM also stated that BYD and other PRC state-owned entities were destroying competitive markets for U.S. rolling stock manufacturing. In part due to AAM's advocacy, Congress enacted a ban on the use of federal transit funds to purchase rolling stock from PRC-owned companies in 2019, excluding BYD from winning valuable contracts. BYD's lawsuit alleged that AAM was engaging in a "malicious, fraudulent, outrageous, and reckless campaign to damage BYD's reputation and brand with false allegations and misleading rhetoric." The complaint cited Paul's and AAM's statements that that BYD was "simply an arm of China's military and government" and "controlled by the Chinese state" and its citation of BYD as a company whose supply chains were linked to Uyghur forced labor in the PRC. AAM prevailed in federal and appellate court, but the case dragged on for two years before the Supreme Court denied BYD's appeal. AAM incurred nearly $400,000 in legal fees, nearly 10 percent of its annual budget. BYD filed a similar defamation suit against the media outlet *Vice*, citing an article linking BYD to Uyghur forced labor and another using the word "blacklisted" to describe U.S. law prohibiting the use of federal funds to buy BYD-made vehicles. *Vice* prevailed in federal district court, and the Supreme Court declined to hear BYD's appeal.

This June, Yangtze Memory Technologies Corp (YMTC), one of the PRC's leading flash memory chip manufacturers, filed a lawsuit in U.S. federal court against the Danish consulting firm Strand Consult and its senior executives. Strand publishes the platform "China Tech Threat." YMTC alleges that Strand Consult illegally asserted that YMTC's chips presented a national security threat. The complaint highlighted several "outlandish and demonstrably false" statements in *China Tech Threat* articles, including a 2022 report co-authored by a Strand executive called "Silicon Sellout: How Apple's Partnership with Chinese Military Chip Maker YMTC threatens American National Security." The report stated that YMTC was a Chinese semiconductor maker with known ties to the PRC military. YMTC maintains that the report and other *China Tech Threat* articles caused it reputational damage. The case is pending.

PRC-based entities have also filed similar libel and defamation suits in Taiwan and France. The Taiwan conglomerate China Times Media Group and its owner food manufacturing conglomerate Want Want, has filed libel and defamation complaints to deter reporting on their close relationship with the PRC. Most prominently, the group sued Financial Times correspondent Kathrin Hille for publishing an article alleging PRC influence over the *China Times*.[26] The conglomerate also sued Taiwan's state-owned Central News Agency for quoting the article. It ultimately rescinded both cases.[27] In 2021, the Taipei District Court dismissed a defamation suit by Want Want's president, Tsai Eng-Meng, against several political commentators and writers for

---

[25] BYD Co. v. All. for Am. Mfg., No. 1:20-cv-03458 (TNM) (D.D.C. Aug. 6, 2021).
BYD Co. v. All. for Am. Mfg. 2022 BL 163199 (D.C. Cir. May 10, 2022), *cert. denied*, 21-7099 (U.S. Aug. 11, 2022) (No. 21-7099).
[26] U.S. Dep't of State, Bureau of Democracy, H.R., and Lab., *Custom Report Excerpts: Taiwan* (2023).
[27] Chien Li-chung and Kayleigh Madjar, *'Financial Times' Defamation Case Dropped*, TAIPEI TIMES, Mar. 12, 2021, available at https://www.taipeitimes.com/News/front/archives/2021/03/12/2003753690

highlighting his close ties to Beijing.[28] Tsai sued another political talk show host for accusing him of promoting PRC propaganda and receiving funding from the CCP to promote Taiwan's reunification with the PRC.[29]

Huawei has also targeted individual researchers for defamation. During Huawei's negotiations regarding access to France's 5G infrastructure, Huawei filed a defamation suit in French court against researcher Valerie Niquet, who had stated on a French TV news program that Huawei is directly controlled by the PRC and CCP. France de facto banned Huawei in 2020, but it was another two years before Huawei withdrew the claim against Niquet.[30]

More research is needed to determine whether libel and defamation suits are being systematically brought by PRC-owned or PRC-based entities against critics as part of a legal warfare strategy. While some of these cases may simply represent zealous advocacy, such litigation would be consistent with the PRC's overall legal warfare strategy to shape an environment favorable for PRC political and economic interests. The PRC and its businesses will be more likely to succeed if their critics are silenced. Even if the PRC does not win its lawsuits, it may succeed in producing a chilling effect on the defendant and other would-be critics, undermining their Constitutional rights.

IV. How PRC Courts' Use of Anti-Suit Injunctions May Harm U.S. Firms and Hinder Due Process

The PRC's own courts have been issuing anti-suit injunctions to prevent foreign patent holders from suing PRC-based companies for intellectual property infringement.[31] These injunctions also enable the PRC to hinder U.S. court proceedings. Anti-suit injunctions, or ASIs, hold plaintiffs in contempt of court and may impose fines for proceeding with parallel litigation against PRC-based entities in foreign courts. In common law jurisdictions, ASIs may play an important purpose in minimizing conflicts of law and preventing cases from proceeding in multiple jurisdictions simultaneously. By contrast, according to the U.S.-China Economic and Security Review Commission's 2023 Annual Report to Congress, ASIs in PRC courts target only foreign litigation and only apply to cases outside of the PRC. Many court decisions involving ASIs have not been published, and ASIs do not have a clear legislative basis. The highest levels of the PRC's political and judicial leadership have promoted the use of ASIs, reflecting the non-independence of the PRC's judiciary.[32] ASIs have been used to drive down the fair, reasonable, and nondiscriminatory (FRAND) royalty rates for standard-essential patents (SEPs) owned by foreign firms. Doing so reduces the cost of foreign technology inputs for PRC manufacturers. PRC courts

---

[28] Jason Pan, *Tsai Eng-meng's Lawsuit for Defamation Tossed Out*, TAIPEI TIMES, Jun. 26, 2021 https://www.taipeitimes.com/News/taiwan/archives/2021/06/26/2003759834.

[29] Taiwan High Court Criminal Ruling 110 Kan-Tze 1058 (2021).

[30] Nathalie Guibert, *Huawei Withdraws Defamation Suit Against a French Researcher*, LE MONDE (July 8, 2022), https://www.lemonde.fr/en/international/article/2022/07/08/huawei-withdraws-its-defamation-suit-against-a-french-researcher_5989403_4.html.

[31] U.S.-CHINA ECON. & SEC. R. COMM., *supra* note **Error! Bookmark not defined.**, at 185-86.

[32] Mark Cohen, *China's Practice of Anti-Suit Injunctions in SEP Litigation: Transplant or False Friend?* in JONATHAN BARNETT, ED., 5G AND BEYOND: INTELLECTUAL PROPERTY AND COMPETITION POLICY IN THE INTERNET OF THINGS, May 31, 2022, at 17.

appear to be using ASIs in an attempt to prevent any jurisdiction in the world other than the PRC from setting FRAND rates.[33] The PRC's use of ASIs employs the legal warfare principle of seizing standards and using them flexibly, in the PRC's interests. The PRC has imported a common law concept and twisted it to thwart due process at home and abroad. The PRC's use of legal terminology accepted by common law systems to justify its actions conveys a sense of legitimacy when its judiciary impedes foreign court proceedings.

V. How the PRC Employs Legal Warfare to Steal Sensitive Technologies and Avoid Judgments

Two other legal sagas illustrate how the PRC and its state-owned enterprises dodge accountability for illegal and malign behavior, attempt to gain access to sensitive technologies, and move assets beyond the reach of U.S. courts.[34] Dallas-based Tang Energy Group's joint venture with the Aviation Industry Corporation of China (AVIC), a PRC state-owned entity, was once the world's second-largest manufacturer of wind-turbine blades. In 2008, Tang, private investors, and AVIC International USA, a California-based subsidiary of AVIC, formed a new joint venture, Soaring Wind Energy. Tang alleged that AVIC then quietly established two new business entities to compete with Soaring Wind. AVIC allegedly funneled funds, assets, intellectual property, and even executives away from Soaring Wind to the new entities, in violation of the terms of the joint venture. Tang and Soaring Wind's other investors filed for arbitration in 2014. The arbitration panel awarded $70 million to Tang and Soaring Wind in 2015, finding that "AVIC HQ exercises such complete dominion and control" over all of its subsidiaries that they "operate as a single economic entity" and were therefore jointly liable. Years of proceedings followed in U.S. federal courts. Meanwhile, the AVIC entities paid nothing on the judgment, which was rapidly accruing interest. Simultaneously, AVIC USA sold off assets and moved its funds outside the reach of U.S. courts. After a federal court confirmed the arbitration award, Tang asked a federal court to order AVIC USA to turn over its remaining assets. On August 10, 2020, the Court found that "AVIC USA has been transferring assets to avoid this Court's judgment." Two months later, AVIC USA filed for bankruptcy, effectively putting on hold Tang's attempts to collect the $85 million it was owed. In January 2022, the parties reached a confidential settlement that allowed Tang to recover only $24 million.

As the PRC scrambles to catch up with the technology of Starlink's low-earth orbit satellite constellation, a PRC-based entity has resorted to courts in the U.S. and Liechtenstein to thwart competitors.[35] The PRC has identified the importance of low-earth orbit satellites as critical to victory in any future military conflict. In 2023, Liechtenstein, backed by Germany, halted a PRC effort to obtain critical broadband satellite frequencies. Shanghai Spacecom Satellite Technologies (SSST) is a military-connected, majority government-owned enterprise established specifically to invest in Western satellite projects. The PRC's five-year plan for 2021-2025, which includes a

---

[33] U.S.-CHINA ECON. & SEC. R. COMM., *supra* note **Error! Bookmark not defined.**, at 185-86.

[34] For representative cases in the Tang/AVIC matter, *see supra* note 4. *See also* Jillian Kay Melchior, *A Costly Lesson in Chinese Business Practices*, W.S.J., Jan. 14, 2022. Jillian Kay Melchior, *A Legal Settlement Shows the Risks of Doing Business in China*, W.S.J., Mar. 14, 2022.

[35] On KLEO/Rivada, *see* Glenn Chafetz and Xavier Ortiz, *China, Lawfare, and the Contest for Control of Low Earth Orbit*, THE DIPLOMAT, Aug. 10, 2023.

directive to acquire the orbital and frequency spectrum, lists SSST as a key partner and tasks it with unifying national efforts to develop low-earth orbit satellite constellations.

Long before that plan was published, SSST appears to have been working to further PRC interests. KLEO, a German/Liechtensteinian company, owns the Liechtenstein rights to three of the highest priority filings with the International Telecommunications Union (ITU), the U.N. agency that manages and deconflicts spectrum priority and flight paths to prevent satellite interference. High-priority ITU filings equate to better orbital slots and transmission frequencies. SSST acquired a 10 percent stake in KLEO in 2017 and proceeded to try to control the company and its ITU filings. SSST acquired a majority voting interest by 2019, creating a split in the company's leadership. SSST and its supporters unilaterally awarded a satellite manufacturing contract to a PRC-based entity, the Shanghai Engineering Center for Microsatellites (SECM). The European-led faction feared this was an effort to turn KLEO and its valuable filings over to the PRC. The German Ministry for Economic Affairs and Climate Action determined a risk that the PRC military would use the satellite constellation "to the detriment of the defense capability of [Germany] and its allies."[36] The SSST also contracted with the PRC government to launch two small satellites under KLEO's auspices. Meanwhile, the SSST appears to have built a shadow effort mirroring KLEO's operations in Shanghai. Soon after, In 2021, the SECM launched two more satellites in the KLEO-owned orbital slot and frequency range.

KLEO's founders then partnered with a U.S. start-up company, Rivada Networks. SSST filed additional lawsuits against Rivada in Liechtenstein, Germany, Luxembourg, and the United States to try to gain control of KLEO's spectrum rights. Liechtenstein regulators rejected the SSST's claim to ownership of the Liechtenstein ITU rights in 2022 and awarded the spectrum rights to Rivada, and this award was backed by Liechtenstein courts. SSST continued to protest. As of September 2023, PRC investors had filed more than 160 lawsuits and arbitration proceedings to obtain the frequencies. Rivada has already incurred $25 million in legal fees, with additional cases still pending.[37]

If the lawsuits to date had gone differently, it could have had a major impact on U.S. national security interests. According to a report in *The Diplomat*, if the PRC had gained control over the Rivada satellite constellation through litigation, 43 low-earth orbit satellites—launched by a majority PRC government-run company that is connected to the PRC military—would be over U.S. territory at any time.[38] At an extreme, driving up litigation costs through spurious litigation can force companies into bankruptcy, allowing foreign adversaries to mine bankruptcy proceedings for national security technologies.[39] A litigation strategy to deplete Rivada's funds would be consistent with the PRC's interest in degrading the development of the U.S.'s national security-sensitive technology. Meanwhile, PRC-backed entities can now also clog up the orbital planes to which they illegally gained access with illicit equipment. A trade bulletin reports that in

[36] David Ignatius, *In Fight Over Satellite Array, Tiny Liechtenstein Roars Back at China*, WASH. POST (Sept. 27, 2023).
[37] Kevin O'Scannlain, Senior Vice President, Rivada Networks, e-mail to Jill Goldenziel, Sept. 12, 2024.
[38] Chafetz and Ortiz, *supra* note 35.
[39] *See generally* Camille A. Stewart, *Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankfuptcy Proceedings*, 10 J. NAT'L SECURITY L. & POL'Y 277 (2019).

February, SSST raised 6.7 billion yuan (almost USD $945 million) for construction of a constellation of 12,000 satellites.[40]

The cases of Tang and Rivada bear detailed explanation because they exemplify how the PRC and PRC-backed entities can use deception and legal warfare to advance PRC military and political interests. While it is not definitively known whether the PRC government backed AVIC, SSST, and KLEO in their lawsuits, AVIC is a PRC state-owned entity, and SSST is majority government-owned and connected to the PRC military. The actions of AVIC, SSST, and KLEO inside and outside of court are consistent with PRC's legal warfare strategy and furthering its national interests. Other examples likely exist, as U.S. corporations are often unaware of the PRC's malign behavior and are vulnerable to PRC influence.

VI. Considerations for Congress

The United States cannot cede the legal and moral high ground to the PRC. It must act decisively to counter PRC-backed legal warfare. The United States's strategy to counter adversary legal warfare is woefully underdeveloped, even compared to its close allies. The Office of the Legal Advisor at NATO's Supreme Headquarters Allied Powers Europe/Allied Command Operations (SHAPE/ACO) has full-time personnel working on countering adversary legal warfare. Israel, too, has personnel in its Ministry of Justice dedicated to countering adversary legal warfare. The U.S. has no counterpart to these programs, in doctrine or in manpower. No agency within the U.S. government has an office or personnel dedicated to countering legal warfare by U.S. adversaries.

Recognizing the threat from legal warfare by the PRC and other adversaries, the U.S. Indo-Pacific Command developed a Counter-Lawfare Program devoted to countering the PRC's legal warfare in 2022. The program includes "reinforcing the current rules-based international order and contesting efforts by potential adversaries to undermine and reshape international law," and to "deny potential adversaries from using 'legal warfare' as a tool for coercion or pretext for aggression."[41] The program, which I advise, has enjoyed great success. Several ally and partner nations have followed suit and adopted counter-lawfare as part of their military efforts. The PRC has expressed ire for counter-lawfare efforts by the U.S. and its allies and partners, particularly the Philippines.[42] The U.S. European Command recently developed a similar Counter-Lawfare Program, and the U.S. Southern Command and U.S. Cyber Command have begun projects devoted to countering adversary legal warfare.

---

[40] Chris Forrester, *Kleo Connect Out of Cash*, ADVANCED TELEVISION, Feb. 5, 2024, available at https://advanced-television.com/2024/02/05/kleo-connect-out-of-cash/

[41] U.S. Indo-Pacific Command, J06 Office of the Staff Judge Advocate, available at https://www.pacom.mil/Contact/Directory/J0/J06-Staff-Judge-Advocate/; *see also* Timothy Boyle, *U.S. Indo-Pacific Command Charts a Course for Countering China's Legal Warfare*, ARTICLES OF WAR, Aug. 20, 2024.

[42] *See, e.g.*, *South China Sea: Chinese Academics Urged to 'Construct Narratives' To Defend Maritime Claims*, S. China Morning Post (June 30, 2024), reprinted in YAHOO NEWS (June 30, 2024), available at https://finance.yahoo.com/news/south-china-sea-chinese-academics-093000616.html (citing Chinese academics and a PRC official discussing the importance of constructing pro-PRC narratives to counter "false narratives" of China's excessive maritime claims circulating in the international community, and expressing rising concern about "rival claimants" "stepping up cooperation with extraterritorial forces" on legal issues).

These efforts, while commendable, are just the beginning of what is needed to effectively counter PRC legal warfare. In addition to supporting these efforts, below are some considerations for what Congress can do to better counter the PRC's threat to the rules-based international order and protect the Constitutional rights of Americans.

1) **Enact Section 1284 of the Senate Draft of the 2025 NDAA on "International Legal Operations."** The Senate Draft of the 2025 NDAA contains a provision called "Report on Department of Defense Role in Supporting International Legal Operations" that represents a vital next step in countering PRC legal warfare.[43] The section, which I helped draft, provides that the Secretary of Defense, working with other relevant federal agencies, will submit a report to Congress on the Department of Defense's role in supporting whole-of-government efforts "to identify and expose the international legal operations of malign actors," to include PRC legal warfare efforts. The legislation appropriately recognizes that countering legal warfare must be a whole-of-government effort supported by the Department of Defense.

2) **Create an Executive Branch Entity Dedicated to Countering Adversary Legal Warfare.** Congress should create legislation to establish an office dedicated to countering adversary legal warfare within the executive branch. The office would serve as the primary subject matter expert on countering legal warfare within the U.S. government, developing a U.S. government strategy to counter adversary legal warfare, and coordinate interagency efforts to counter legal warfare. I have written in detail elsewhere about the functions and duties of such an office.[44]

3) I**nvestigate, Monitor, and Research PRC Legal Warfare Efforts.** Investigating and monitoring PRC legal warfare efforts and raising awareness of them is one of the most important things that Congress—and especially this Committee—can do to counter it. Much research is needed into the existence and extent of the PRC's legal warfare efforts, particularly those occurring in U.S. courts and within U.S. borders. Care must be taken to distinguish zealous advocacy efforts by U.S. lawyers using our legal system in standard ways from systematic, PRC-backed efforts to undermine U.S.-based litigation proceedings and commit illegal acts.

4) **Support Counter-Legal Warfare Training, and Education**. Besides the investigative powers of Congress itself, Congress can fund and support research into efforts to counter legal warfare by entities within the federal government and/or private universities, as well as training and education on countering legal warfare. For example, Congress might consider supporting additional research, training, and education efforts at National Defense University's College of Information and Cyberspace, which has faculty who are experts in all of the PRC's Three Warfares. The National Defense University is also well positioned to provide reach-back support and training on countering legal warfare to the Joint Force and civilian agencies, to provide in-depth research on countering legal warfare to support their efforts, and to conduct international engagements on countering legal warfare with officials from ally and partner nations. Professional Military Education institutions, federal researchers, or other universities can also support U.S. Combatant Command Counter-Lawfare efforts by conducting research

[43] U.S. Senate Armed Services Committee, *supra* note 6.
[44] Goldenziel, *Law as a Battlefield*, *supra* note 1, 1162-1171.

on PRC legal warfare efforts that transcend the area of responsibility of any one geographic or functional Combatant Command. Establishment of a NATO Center of Excellence to counter legal warfare could be another option for centering U.S. government counter-lawfare research, training, and education efforts. Working with NATO would also provide valuable coordination with U.S. partners and allies.

In addition to supporting U.S. government and military efforts, research on the extent of PRC legal warfare is also necessary to empower litigants to use sanctions available in federal courts to deter PRC legal warfare. The primary instrument to deter and punish frivolous lawsuits in U.S. federal courts is via "Rule 11 sanctions," named for the corresponding Federal Rule of Civil Procedure. However, judges are often reluctant to grant Rule 11 sanctions, and may be especially reluctant to do so against foreign sovereigns and state-owned entities so as not to interfere with foreign affairs, generally seen as the province of the Executive and Legislative branches. Likewise, Congress must be careful not to interfere with the autonomy of the judiciary or judicial decisions, or the due process rights of litigants. Congress can, however, designate and/or fund an executive branch agency, Professional Military Education institution, or independent university or organization to document litigation by PRC-based entities in U.S. courts, with the goal of determining whether litigation is part of a PRC-backed legal warfare strategy. This entity can also educate litigants about the potential risk of legal warfare. Judges will be more likely to grant Rule 11 sanctions in the face of systematic evidence that the lawsuits are vexatious.

5) **Enact a federal anti-SLAPP Statute**. Congress might also consider a federal Anti-SLAPP statute to assist with dismissal of claims designed to punish critics of the PRC for exercising their First Amendment rights.[45] While a number of states have Anti-SLAPP statutes, no federal Anti-SLAPP legislation exists. Anti-SLAPP statutes provide that alleged victims of SLAPP lawsuits can file a special motion that would allow the court to quickly dismiss the suit. The defendant bears the burden of showing that they are being sued for exercising Constitutional rights. If they meet this standard, the plaintiff then must show that it will prevail on the merits of the case in order for it to proceed. Anti-SLAPP statutes typically expedite judicial considerations of the anti-SLAPP motions, stay discovery, provide attorney's fees for the defendant if it prevails, allow for immediate appeal, and provide penalties for filing the claims as well as additional relief required to deter the vexatious conduct. A federal anti-SLAPP statute, carefully drafted to protect due process, could help deter frivolous legal claims by PRC-based entities.

6) **Ensure that investors know their rights and risks.** Congress can help ensure that investors understand their rights and protections when doing business with the PRC, and how they may differ from doing business with other entities and provide knowledge of how investors can protect themselves. Doing business in the PRC is different than doing business in other foreign entities due to the PRC's laws and the foreign investment treaty between the U.S. and PRC. The U.S. and the PRC do not have a bilateral investment treaty. The U.S.-PRC Foreign Investment Treaty dates to 1985, a time when the PRC was just starting to develop economically and open its markets to the world. The treaty contains basic terms such as fair and equitable treatment but provides few protections for intellectual property. Until the U.S.

[45] *See generally* Diego Zambrano, Testimony Before the U.S.-China Economic and Security Review Commission, May 4, 2023, available at https://www.uscc.gov/sites/default/files/2023-05/Diego_Zambrano_Testimony.pdf.

can improve treaty protections for its businesses, Congress can help investors understand the risks of doing business in and with the PRC.

VII. Conclusion

The PRC is not afraid to weaponize U.S. laws and the U.S. legal system. The U.S. must fight back—with some caution. The United States cannot compromise judicial independence; nor can it compromise the due process rights of U.S. persons. Our own commitments to due process and the rule of law must not be tarnished by the PRC's disregard of the same. Congress should consider passing legislation to counter legal warfare, establishing a lead entity to develop and execute strategy to counter legal warfare, investigating and monitoring PRC legal warfare efforts, supporting research, education, and training on countering legal warfare, and raising awareness of the PRC's attempts to undermine the international and constitutional order. By doing so, Congress will improve protections for U.S. businesses and national security interests. Understanding how the PRC is weaponizing the U.S. legal system will also empower U.S. firms and individuals to protect their rights.