SHIELD
by SOURCEREE

What's Inside

CFIUS Newsletter

November 2020

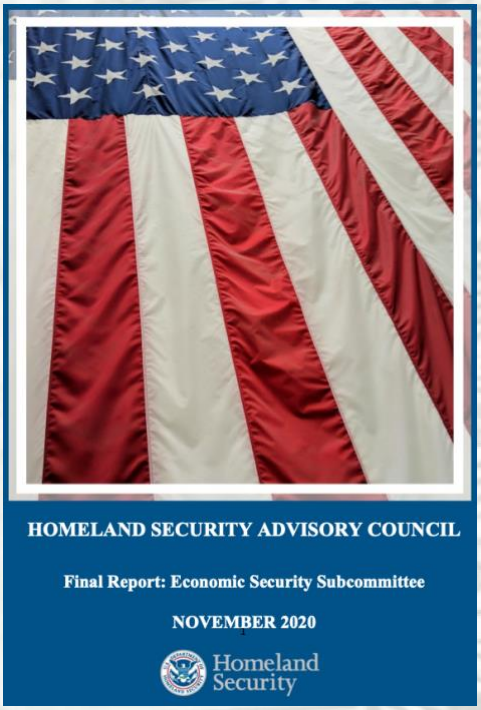
SOURCEREE

Authors: Adam Murphy & John Lash

DHS: Economic Security Final Report

This report sought to address the question: How can the Department of Homeland Security (DHS) contribute to the goal of greater economic security?

In reviewing the report, we elected to excerpt sections specific to CFIUS which provide details and recommendations that should be considered throughout government in order to bring forth appropriate solutions.



Select excerpts from the report:

The Treasury Department administers and chairs CFIUS. CFIUS was created in the 1970s to address the special risks created by foreign investment in certain American industries. Foreign investment in the U.S. is usually welcome but it can sometimes pose a real threat to economic security. Companies based in adversary countries, whether they are nominally private or state-owned enterprises, may buy U.S.-based technology companies and move that technology out of the U.S. permanently. Indeed, as the Defense Department has learned, these transactions do not have to be outright purchases. They can include many joint ventures and equity investments as well. Many such transactions were beyond the reach of CFIUS until the adoption of FIRRMA. FIRRMA strengthened CFIUS's authorities to reach joint ventures, police transfers of critical technology, and mitigate risks through national security agreements.

That said, CFIUS by itself still cannot address all threats to U.S. economic security.

- For one thing, it covers investments in U.S. companies.
    - **It does not deal with foreign companies that build their businesses in the U.S. from scratch, either through investment here or through imports.**
- Second, CFIUS exists to shine an intense spotlight on a single transaction by a single foreign buyer at a single point in time, and its only recourse is to prohibit or limit that particular acquisition.
    - **In many cases, a broader view of the industry and global competition is necessary to appreciate the risk and to fashion a remedy more effective than just saying "no" to the deal at hand. We believe that conducting such a broader review is one valuable role that DHS's economic security unit should undertake in the future.**

The DHS Policy Office has taken the lead in developing requirements for supply chain mapping and should be commended for its willingness to devote resources to the issue. Like CISA, it has a sustained history of engagement with economic security issues. Its CFIUS and Team Telecom unit has long been among the federal government's more determined advocates for protecting the nation's civilian information and communications infrastructure from risky foreign influence.

The Policy Office has now combined its nascent economic security capabilities with its established CFIUS and Team Telecom staff under a Deputy Assistant Secretary for Economic Security. We support this organizational structure, which reinforces the significance of the issue and allows the transactional expertise of the CFIUS and Team Telecom staff to be deployed on a wider scale. **There is a clear need for a political-level policy official to conduct day-to-day policy coordination and representation of the Policy Office, both at the interagency level and in working with CISA.**

While combining the economic security unit with the CFIUS and Team Telecom unit makes sense, more capacity is needed. Currently, the Policy Office focuses on economic security in the context of single transactions, usually with a 45-day deadline. Such decision making can produce focused and prompt resolutions, but it does not deal well with broader supply chain issues, such as competitors who expand organically rather than through acquisition, or who have received state assistance in the form of subsidies or cyberespionage support. CFIUS cases are enormously valuable in identifying a supply chain problem but they rarely provide a complete solution to the problem they uncover. **To go beyond individual cases to more strategic assessments and solutions will require more resources, and perhaps substantially more resources.**

Another way for DHS to expand its economic security capabilities is to build on a foundation laid by CFIUS and Team Telecom. It often occurs that a CFIUS or Team Telecom matter exposes a vulnerability not previously understood. But these authorities only allow the government to permit or veto a particular transaction. **Often, though, the transaction simply brings to light a much broader supply chain problem; a wider study of the industry and of remedial actions is frequently needed.**

DHS Report: https://www.dhs.gov/sites/default/files/publications/final_economic_security_subcommittee_report_1.pdf

Report focuses first on the challenge posed by adversary nations hoping to use economic interdependence against the United States. It then provides an overview of the work already being done in other U.S. government agencies on economic security issues and how DHS can assist them. Finally, the report takes a closer look at how components of DHS are working the issue.

Secretary of State: The China Challenge

This report provides context for the new era of great-power competition between China and the rest of the world, specifically the United States.

The State Department report details vulnerabilities of the intellectual sources which the People Republic of China (PRC) has established for authoritarian rule: constraining innovation, difficulty forming and maintaining alliances, costs arising from internal repression, economic instability, demographic imbalance, environmental degradation, and a disregard for international norms and obligations.

For the US to meet the China challenge, ten foreign policy tasks were recommended.

Select excerpts of the report:

- **China engages in massive intellectual-property theft.** The PRC has perpetrated the greatest illegitimate transfer of wealth in human history, stealing technological innovation and trade secrets from companies, universities, and the defense sectors of the United States and other nations. According to research cited by the Office of the United States Trade Representative, China's efforts — including forced technology transfer, cyberattacks, and a whole-of-nation approach to economic and industrial espionage — cost the U.S. economy as much as $600 billion annually. This staggering sum approaches the Pentagon's annual national defense budget and exceeds the total profits of the Fortune 500's top 50 companies. All 56 FBI field offices are conducting China-related economic-espionage investigations across nearly every industrial sector
- **China pursues control over key international supply chains and essential materials and goods.** Since Beijing's controversial 2001 accession to the World Trade Organization, U.S. multinational companies have relied increasingly on the PRC's low-cost labor force to produce and export cheaper finished goods, especially in high-technology and advanced manufacturing sectors. This shift resulted in lower prices for U.S. consumers and higher profits for U.S. companies. Among the costs, however, was a "China Shock" that devastated small- and medium-sized manufacturing in the United States and other nations, wiping out as many as 2.4 million jobs in America alone and leaving crucial international supply chains dependent on China. The global pandemic has thrown this supply-chain vulnerability into sharp relief.
- **China seeks worldwide industrial dominance, particularly in critical high-tech sectors.** While manufacturing superiority proved decisive in U.S. victories in World War II and the Cold War, the United States lost that advantage in many essential industries. For example, China today accounts for 50 percent of global steel and aluminum production, 70 percent of consumer electronics manufacturing capacity, 90 percent of consumer drone production, 45 percent of shipbuilding production, and, by 2022, will likely account for 35 percent of the world's integrated-circuit fabrication capacity. By 2022, China and Taiwan are set to house 70 percent of global capacity for integrated-circuit fabrication, including virtually all cutting edge production, which is vital to the digital economy, advanced weapons systems, aerospace, artificial intelligence (AI), robotics, and other essential industries.

- **China aims to build the world's fifth generation (5G) wireless-telecommunications physical and digital infrastructure as a steppingstone to broader dominance in emerging and next-generation information technologies.** Beijing heavily subsidizes state-directed Huawei and ZTE, enabling these telecommunications behemoths to undercut rivals in the race to construct 5G networks on every continent. Since Huawei and ZTE are subject to China's various national security laws that compel them to "support, assist and cooperate with the state intelligence work," countries that use them as 5G vendors face growing threats to their network integrity, data privacy, economic stability, and national security.
- **The CCP uses the Belt and Road Initiative (BRI)** — originally called One Belt One Road (OBOR) and still so designated by the PRC in Chinese-language sources — and other undertakings to expand foreign markets for Chinese companies and as a means of drawing nations, particularly their political and economic elites, into Beijing's geopolitical orbit. BRI infrastructure projects — ports, railroads, highways, dams, industrial parks, civil nuclear facilities and other energy related initiatives, and more — typically rely on imported Chinese workers rather than local labor, and sometimes involve 50- to 100-year business relationships that entrench China's long-term access to local elites and confer power over key parts of the host country's critical infrastructure. Because of the heavy economic and environmental costs imposed by the CCP, host countries increasingly find these BRI projects unsustainable
- **China leverages often unfettered access to foreign capital markets.** In particular, U.S. stock exchanges today list over 130 Chinese companies — including Alibaba, PetroChina Company Limited, China Life Insurance Company Limited, China Petroleum & Chemical Corporation, Baidu, and Tencent — with a combined valuation of over $1 trillion. Following massive financial and accounting scandals in the early 2000s, the U.S. Congress enacted laws requiring regulators to inspect the audits of all U.S.-listed companies. China is the only country that invokes its state security laws to block U.S. regulators from conducting these inspections. Moreover, U.S. investors and pension holders unwittingly pour billions into managed funds that invest in Chinese companies that are listed on exchanges outside the United States. Moreover, some foreign-listed Chinese companies — including Hikvision, Dahua Technology, and the weapons-manufacturing subsidiaries of Aviation Industry Corporation of China — have ties to Beijing's military modernization, espionage, and human rights abuses, and may be subject to U.S. sanctions and export controls.

State Report: https://www.state.gov/wp-content/uploads/2020/11/20-02832-Elements-of-China-Challenge-508.pdf

Along with knowledge of China's conduct and its intellectual sources, understanding of the CCP's vulnerabilities — not least the limitations of its ability to address its vulnerabilities — must inform U.S. efforts to meet the China challenge.

CNA: Economic Statecraft

Through this report, the Center for Naval Analysis (CNA) provides an overview of the legal economic tools that the People's Republic of China (PRC) uses to obtain foreign technology and build capabilities in support of China's national security objectives.

The PRC pursues its national security objectives through a wide variety of cross-domain activities. While China's legal economic-statecraft activities are used to advance it's growing military power, the outcome is directly impacting the technological superiority of the United States and its citizens and allies.

Select excerpts of the report:

- **China uses a multifaceted approach to develop defense capabilities that fuses both legal and illegal acquisition of foreign technologies, reverse engineering, and indigenous production. Some key aspects of this approach include:**
    - Acquiring technology from foreign countries to provide China with a model to study, test, learn from, and then replicate.
    - Reverse engineering foreign weapons or technology in order to build China's own indigenous capability.
    - Integrating civilian and military sectors, allowing China to repurpose civilian technologies into military capabilities.

Many of China's tools for acquiring foreign technology are legal.

  - Although China has engaged in illegal activities to support its military modernization, the PRC uses a wide range of legal economic tools at its disposal.
- **China's targets for technology acquisition are tied directly to PRC national strategic objectives.**
  - Publicly available PRC government planning documents, such as Five-Year Plans and Made in China 2025, identify priority industries and capabilities for development, including advanced technologies such as aerospace, biotechnology, and maritime equipment. China's state-driven effort to fuse civilian and military resources to achieve PRC national security goals complicates US responses.
- **The stakes are high for the United States and its partners and allies. China's legal economic statecraft activities are directly connected to the PRC's growing military power—and to other countries' loss of technology and intellectual property (IP).**
  - China's ability to access critical technology could erode the technological superiority of the US military and the defense industrial base of the US and its partners and allies.
  - Countries at the leading edge of scientific and defense research are vulnerable to having their IP accessed through a wide range of PRC economic activities.

CFIUS: The impact of heightened scrutiny of Chinese investments in US companies

In response to these and other changes in the international investment environment, China has diversified its investment tactics to avoid increasingly strict investment barriers and gain access to "encouraged" industries in foreign countries.

Over the past decade, China has increasingly relied upon indirect vehicles to invest abroad. Multinational corporations often use creative ownership structures to diversify their investments or avoid taxes. The Organization for Economic Cooperation and Development (OECD) defines these various investment groups as "special purpose entities," which include investment funds, private equity and venture capital funds, holding companies, or other types of legal "shell" companies. These special purpose entities have been especially helpful for Chinese firms seeking to invest in US firms while not triggering US investment controls

PRC-backed equity investment funds are an increasingly prominent tool for China's attempts to acquire foreign technology. Government-backed equity investment funds pool resources from across the PRC government bureaucracy into one fund intended to serve a dedicated purpose. These investment funds typically support startups and non-publicly traded companies in a specific sector. The Chinese government has encouraged the use of government-financed industry-specific investment funds to support national economic development priorities and policies, such as the MIC 2025 policy. As of March 2018, over 1,800 such funds were in existence. The US-China Business Council has noted, "As part of military-civil fusion, Chinese firms obtain dual-use technologies through overseas acquisitions supported by government funding." These financing vehicles have a variety of corporate structures, comprise a large number of shareholders, and often use holding companies.

Illustration: Linking acquisitions to government priorities

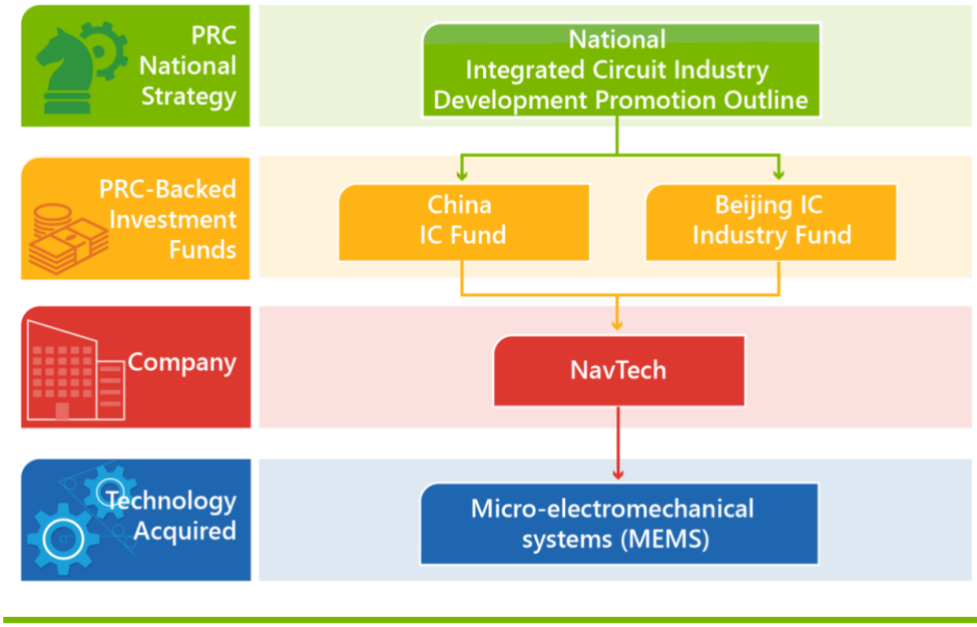
China's acquisition of Silex Microsystems, a Swedish firm, provides one example of how the PRC uses indirect investment techniques to target specific foreign companies in the service of publicly stated PRC national strategic goals. This example also illustrates the challenges of regulating dual-use technology.

In 2016, an apparently private Chinese company, NAV Technology Company Limited (NavTech), acquired the Swedish-based Silex Microsystems. Silex specializes in developing and manufacturing micro-electromechanical systems (MEMS), a crucial component inside the chips embedded in most electronic devices. Although not immediately apparent, NavTech maintains close ties to the Chinese state and military. Thus, in agreeing to this acquisition, "Sweden may inadvertently assist the Chinese military in modernizing its capabilities."

The Silex case illustrates the links between PRC government priorities and the targeting of specific foreign firms for acquisition. For example:

- PRC guiding national strategies, such as the National Strategic Emerging Industry Development Plan and the National Integrated Circuit Industry Development Promotion Outline, emphasize China's need to develop MEMS and integrated circuit (IC) technology.
- In 2014, the PRC pooled resources from across several SOEs to establish the China National Integrated Circuit Industry Investment Fund (China IC Fund). Two PRC government agencies also jointly established the Beijing Integrated Circuit Industry Development Equity Investment Fund (Beijing IC Industry Fund). Both of these PRC-backed private investment funds are tasked with providing capital for the R&D of integrated circuitry.
- According to NavTech's website, these two funds are its second- and third-largest investors.
- Likely unknown to Silex, NavTech maintains ties to the Chinese state and military. NavTech's parent company, Beijing Naiwei Times Technology, has received multiple certifications from the PLA for engaging in military R&D, production, and sales.

Figure 7. Linking China's national strategic guidance to technology acquisition targets using indirect investment vehicles



Source: Derived from "NavTech Participates in the Investment of Beijing IC Industry Fund."

Illustration: Combining tactics to access US technology

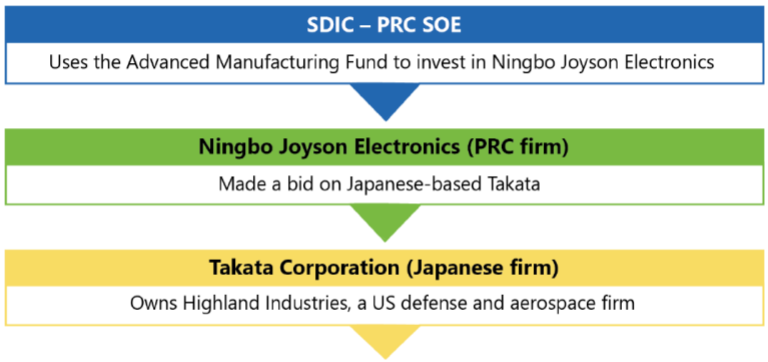
A recent case involving China's State Development and Investment Corporation (SDIC) illustrates two trends in China's investment toolkit: use of indirect investment vehicles and investment via third countries. SDIC is a SASAC-controlled, state-owned enterprise created in the mid-1990s that manages a variety of SOEs and other types of investment funds meant to target the "advanced manufacturing industry." Many of SDIC's subsidiary organizations are responsible for undertaking goals associated with MIC 2025.

SDIC used one of its investment funds to invest in Ningbo Joyson Electronics, a privately owned automotive components manufacturer based in Ningbo, China. In 2017, Ningbo Joyson Electronics announced that it would attempt to acquire the Japanese firm Takata.

Takata Corporation owns several US firms, one of which, Highland Industries, specializes in composite materials for the defense and aerospace industry, including "rocket components, satellite components, munitions tubing, protective gearing," and other materials.

Thus, through this deal, Chinese state-owned and private firms could potentially gain access to technology associated with Highland Industries. As of April 2018, the purchase of Takata was complete with the new, combined company called "Joyson Safety Systems." The new consortium remains owned by the Chinese parent firm but will be "based in Michigan."

Figure 8. SDIC's pathway of technology access



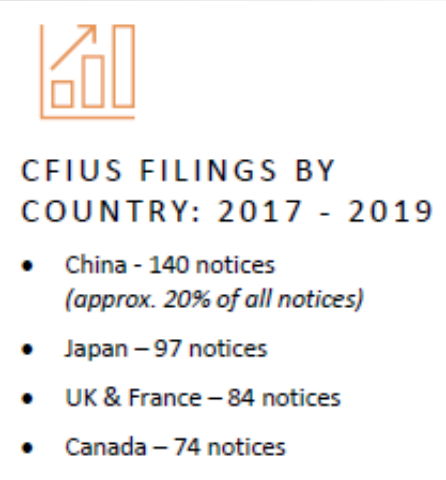
Source: Derived from Highland Industries, "Highland Composite Structures"; *Automotive News*, "China's Ningbo Joyson Considers Bid for Takata Following Key Safety Acquisition"; SDIC Fund Management, "Advanced Manufacturing Industry Investment Fund," http://www.sdicfund.com/. See endnotes for full citations.

CNA Report: https://www.cna.org/CNA_files/PDF/DRM-2020-U-027240-1Rev%20(002).pdf

Approved for public release. Work performed under Federal Government Contract No. N00014-16-D-5003

Lash PhD Research: CFIUS Game Theory

In October 2020, John Lash successfully defended his PhD thesis - *The Feasibility of Game Theory Approaches: An Investigative Study of Threats to US National Security from Foreign Investment.* The research focused on the convergence of trade policy, economic espionage, and national security.



Abstract:

The goals of this report are twofold. The first goal is to explain how the key variable of national security impacts foreign direct investment in the United States. The second is to fill an important gap in the literature on the Committee on Foreign Investment in the United States (CFIUS) by offering a detailed conceptualization of how national security and trade policy converge, including the development of a modern pure-conflict game theory model.

United States national security reviews have a material impact on foreign direct investment, with second and third order consequences not fully vetted by extant research.

As the world economy continues to shrink due to globalization, the United States must consider the development of a modern game theory investment security model to address the complex convergence of economic modernization and the national security impact of foreign direct investment.

This research identifies and outlines critical observations and implications for policymakers to establish stable national security and growth oriented economic policies.

More to come in future Newsletters!

Research brief is available on request. We would welcome the opportunity to provide a full debrief to any interested agency.

Protected by

SHIELD by SOURCEREE

Sourceree's SHIELD program is a comprehensive supply chain risk management (SCRM) solution designed to help answer questions about supply chain disruptions and risks, particularly foreign investment.

SHIELD VISION

Software platform for on-demand supply chain risk assessments and financial intelligence

SHIELD SQUAD

Analytical Support

SHIELD INTEL

Business intelligence reports on critical suppliers