Introduction

Over the summer of 2015, the popular national security blog “Lawfare” asked readers to name the most hackable database operated by the United States government. The request came in the wake of a massive Office of Personnel Management database hack in spring 2015. The primary authors and readers of Lawfare submitted dozens of potential databases, mostly involving various types of information about government personnel.¹

Two of the databases, however, made a different kind of sense. One, proposed by Ben Wittes, was the Commerce Department’s database of export control applications, which determine how and where US firms can export sensitive “dual use” technology.²

² ibid.

Key words: military technology, diffusion, cyberespionage, intellectual property, China
The second, suggested by reader Jonathan Lichtman, was the US Patent and Trademark Office database, which includes applications, with supporting materials, for US patent protection.3

Given the long history of suspected and confirmed industrial espionage on the part of the People’s Republic of China (PRC), both of these databases would make apt targets. Indeed, the available evidence on Chinese cyber-espionage efforts suggest that the People’s Liberation Army (PLA) has focused on US and European intellectual property (IP), with a particular concentration on IP in the defense sector.

This article examines illegitimate diffusion of military technology through the theft of draft patents and trade secrets through cyber warfare. During the Cold War, both the United States and the Soviet Union dealt with concerns about illicit foreign appropriation of military technology, some of which occurred through review of IP documents. In the post-Cold War context, these concerns have intensified, as the expanding use of IP has offered a window—sometimes one left wide open—for theft. This is particularly the case for dual-use technology, which is less likely to have been initially created with secrecy protections in place. In recent years, various sources (including the US government and several private firms) have accused China of appropriating a vast amount of IP from the United States, much of it related to military affairs. Of course, China engages in old-fashioned face-to-face espionage. But as the digital age has matured, there is persuasive evidence that China is taking advantage of the steps involved in others’ IP regimes, by using cyber espionage to access into materials developed as part of the IP legal regime. These include defense contractors’ internal legal documents, law firms’ written evaluations of technology, as well as patent applications submitted to the Patent and Trademark Office. The frequency of attack against these access points suggests that states continue to overlook their significance. The opportunity that these access points provide adds a new layer to the analysis of the diffusion of military technology.

IP and Military Technology

Why concentrate on IP law? Historically, the security studies subfield has paid little attention to development in international or domestic IP law, beyond a comment here or there about how technological innovation requires a sound legal basis.4 Few studies, however, have focused on how legal foundations affect a military–industrial complex or how the emerging international IP regime might affect the diffusion of military technology.5

---


But there are now several reasons to believe that IP law, both in its domestic
development and in the context of the emerging international IP regime, may be
having a strong, independent effect on the way states innovate and on how those
innovations find their way around the international community.

First, political demands of defense contracting have grown steadily more
complex. Arms export agreements have increasingly taken on the character of
transnational public–private partnerships. To sell fighter jets, US firms have to agree
to build components in the customer country, as well as to transfer technology
associated with the weapon system. This creates the need for intricate legal
arrangements that delineate where and how firms can transfer technology.

Second, alliances between defense firms have become ever more important
to the production and development of military technology. James Hasik notes in
Arms and Innovation that many of the best-known military systems of the last
decades have emerged from alliances between large, traditional defense producers
and small, nontraditional firms. These alliances inherently create the potential for
conflicts over the ownership of technology and trade secrets, both between the
firms themselves and between the firms and the government. To the extent that the
nature of IP law affects the prospects of these alliances, it has an impact on military
innovation.

Third, the importance of dual-use technologies, especially in the computing
and communications sectors, has complicated the relationships that firms have with
the government. While most firms like selling to the government, few nontraditional
providers envision the Defense Department as their only customer. Rather, they
plan to sell their technological innovations on the open market—hence, “dual use.”
State interest in acquiring the IP rights to the data, patents, and trade secrets of firms
developing dual-use technologies runs directly counter to their commercial efforts.

Finally, private firms have, over the past five decades, committed an
ever-increasing percentage of total funds devoted to technological research and
development. At the same time, the government remains deeply involved in most
defense research, committing substantial resources to the development of new
weapon technologies. Most new systems, consequently, involve some mix of state
and private funding. This creates problems for the ownership of the IP associated
with technological innovations, problems that IP law can either solve or exacerbate.

While the broader project this article is associated with examines the role
of IP law in both diffusion and innovation, this article concentrates on the former.
Specifically, it examines how developments in IP law may have changed the nature
of industrial espionage, especially in cyberspace. The article hopes to develop a
framework for understanding the relevance of the efforts of the PLA to target the IP
of defense-related firms in the United States and Europe.

---

6 James M. Hasik, Arms and Innovation: Entrepreneurship and Alliances in the Twenty-First-Century
Defense Industry (Chicago, IL: University of Chicago, 2008).
The Diffusion of Military Technology

The literature on diffusion in military affairs focuses on three questions. As characterized in the Davis and Eliason edited volume *The Diffusion of Military Technology and Doctrine*,

“The first debate concerns how one defines the diffusion process, which is critical for identifying whether or not diffusion has occurred. The key question here is whether the communication of information is sufficient to conclude that diffusion has taken place... The second debate concerns the causes of diffusion. What motivates states to adopt innovations from abroad, and what is the mechanism by which knowledge is transferred? While scholars advance various typologies, three distinct processes—competition, socialization, and coercion—drive the spread of policies across societies with different implications for what is modeled. The third debate concerns the patterns and effects of diffusion.”

This study concentrates on the second of these three questions, the motivations and mechanisms of diffusion. Previous studies on why and how states seek to acquire technology have concentrated on material factors, organizational factors, and sociological factors. On the materialist pole, Joao Resende Santos argues the neorealist case for military diffusion. States adopt new doctrines, organizational modes, and technologies out of concern for their security, with adoption succeeding insofar as states can devote sufficient resources to the project. In *The Diffusion of Military Power*, Michael C. Horowitz takes an organizational perspective to extend this case, arguing that differences between wealth and organizational complexity limit the diffusion of military power.

Sociological explanations for institutions and behavior presuppose that humans live within a universe of social meanings. Although interest plays a role in behavior, appropriateness and legitimacy help construct the conditions under which states interpret interest. The behavior of others, especially powerful states, legitimates some behaviors and delegitimates others. Norms and expectations structure how states pursue their interests. Several scholars have applied this logic to procurement. Emily Goldman has explored how the impact of the Western military model differed in Japan.

---

and Ottoman Turkey, and Theo Farrell has studied the effect of world military culture on the constitution of the Irish army. Particularly relevant for this study, Dana Eyer and Mark Suchman established that poor countries buy expensive weapons, even when cheap weapons would better meet their needs. Similarly, Daniel W. Henk and Marin R. Rupiya argue that symbolic logic drives much procurement strategy in African states.

Mechanism: Industrial Espionage

This study seeks to meld sociological and materials logics of diffusion. The sociological framework allows that consequential and social logics interact, but specifying how, and under what conditions such interaction produced varied outcomes, is worth the effort. Ideas matter, and the presence of powerful ideational forces at the systemic level can cause states to redefine their identities and change the methods through which they pursue power.

In this study, we argue that a developing configuration of law and technology has made possible a new form of industrial espionage and that this form lies at the center of the struggle between China and the United States over the diffusion of military technology.

As mentioned in the introduction, one means of violating IP rights in the military sphere comes from the reverse engineering of technology acquired through legitimate or illegitimate means. As a practical matter, reverse engineering foreign technology for domestic production faces several difficult obstacles. The thief needs to match, or come close to matching, the industrial and technological sophistication of the target. Taking apart an F-16 to figure out how it works is of no help if the thief cannot produce the components in question.

The appropriating state lacks trade secrets associated with the manufacturing of the system. At the very least, this can make the replication of foreign systems a costly and time-consuming process, as the appropriator needs to develop manufacturing procedures from scratch. At worst, it can lead to seriously substandard components that reduce the capabilities and reliability of a system. For example, Chinese efforts to

---


reverse engineer certain Russian jet engines during the 1990s and 2000s invariably produced engines with extremely short lifespans and without the power of their Russian counterparts.\textsuperscript{16}

Generally, the appropriator also lacks data associated with design and testing. Modern weapon systems generate an extraordinary amount of data during the development process, as computer models explore a vast array of scenarios with respect to potential components.\textsuperscript{17} The testing process also generates data and the appropriating country generally lacks access to prototype models. The appropriating state generally lacks access to testing data associated with the system, which makes it difficult to come to solid conclusions regarding the tolerances of particular materials, or even the purpose of certain subcomponents.

Altogether, reverse engineering an entire system is generally more trouble than it is worth. States which have the industrial and technological capability to reverse engineer a complex system generally also have the capacity to engage in their own design work. Domestic designs mean that the builder can focus on weapon characteristics that it wants, rather than settle on a system designed by a foreign producer.

In some cases, however, reverse engineering makes sense. The difficulty of reverse engineering depends on the gap between industrial capabilities of the target and the appropriator and the amount of information that the appropriator has acquired. If the former is sufficiently small and the latter sufficiently large, an appropriator can profitably do the work necessary to copy a system or at least a group of subsystems.

In the case of cyber espionage, the evidence indicates that China's PLA has targeted exactly these kinds of systems. Instead of copying entire weapons, the Chinese have won access to data on the subsystems that give US weapons their lethality. These include “dual use” technologies that the United States has historical sought to prohibit from export. In addition to US government sources, Chinese hackers have targeted law firms, private corporations, foreign partners, and various intermediaries that possess access to data regarding dual use and military-only technologies.\textsuperscript{18} Although the extent to which such data has found its way into Chinese systems remains uncertain, IP protection has become a central front in cyber conflict between the United States and China.


Cyber Conflict

Many studies have explored the founding of the internet, and the parallel growth of legitimate and illegitimate internet traffic. Over the past decade, however, scholars and policymakers have increasingly concentrated on the prospects for and implication of “cyber conflict,” which amounts to organized conflict between groups in cyberspace. This analysis has given good reason to suspect that cyber warfare differs from traditional warfare in consequential ways.

In *Cyber War versus Cyber Realities*, Brandon Valeriano and Ryan Maness define cyberspace as:

> the networked system of microprocessors, mainframes, and basic computers that act in digital space. Cyberspace has physical elements because these microprocessors, mainframes, and computers are systems with a physical location. Therefore, cyberspace is a physical, social-technological environment—a separate domain but one that interacts and blends with other domains and layers.

They further define cyber conflict as:

> the use of computational technologies for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between states.

According to Valeriano and Maness, almost half of all cyber incidents involve theft, in which one state attempts to appropriate some kind of information from another. In context of this paper, cyber conflict occurs when one state attempts to appropriate IP under the legal protection of another; this is to say, when a state or the agents of a state use access to digital space in order to steal legally defined property.

The concurrent development of cyberspace and the expansion of intellectual property law have changed the context in which states conduct industrial espionage. The digitization of knowledge means that patent applications, trade secrets, and reams of industrial data have become available to talented hackers and dedicated organizations.

---


21 Ibid., 21.

22 Ibid., 9.

Moreover, the functioning of intellectual property law in the United States (and elsewhere) requires a degree of communication between different organizations. The military services, contractors, subcontractors, defense firms, and law firms all have some degree of access to crucial secrets.

In a sense, the vulnerability arises from changes in the nature of the defense industrial complex, and more broadly of modern capitalism. Specialization of firms increases inter-firm communications, which then creates communications vulnerabilities. Cooperation with the regulatory state complicates the picture even further. Many companies and legal firms have already begun to take steps to manage their vulnerability, including developing firewalls on communication with Chinese clients and affiliates. However, hackers have the luxury of concentrating on the weakest links.

Scholarship on the development of the information economy has long grappled with the shift from an industrial to a post-industrial, knowledge based economy. Modern computing technology has enabled the collection of tremendous amounts of data, with processors allowing for search and analysis, and communications equipment facilitating near instantaneous transfer of information. Decades ago, the information contained in the databases mentioned above resided in huge warehouses, and could not effectively be “stolen” without immediate physical presence and the use of heavy equipment.

Cyber Security and the Public Private Bridge

Secretary of Defense Ash Carter elaborated on the Defense Department’s view of cyber security clear in an April 2015 speech at Stanford University. The location was not accidental, as the speech concentrated on the need for cooperation between the Pentagon and Silicon Valley. Carter argued that civilian innovation goes hand in hand with government action on cyber security. This relationship has four aspects:

1. The increasing role that civilian investment plays in military technological innovation demands closer ties between the Department of Defense (DoD) and the centers of civilian innovation.
2. Government investment and support have facilitated the development of many of the technologies central to digital innovation over the past several decades.


(3) Private firms and the government face different facets of the same cyber security problem, as espionage threats target both private and public sector entities.

(4) Private cyber security and publicly provided cyber security overlap; the defense of each depends on the security of the other, as both can come under attack, and vulnerabilities in one sector can lead to vulnerabilities in the other.

Yet some argue that the public–private partnership that interests Carter is particularly unlikely to develop in the tech sector.26 Despite the critical role that government (and DoD) investment played in the foundation of the computing industry (and of the internet), technology firms and their workers tend not to share the values of the military–industrial complex or have much interest in securing government contracts. The Pentagon, operating under government employment restrictions, cannot compete with Silicon Valley salaries. Moreover, the revelations of Edward Snowden exacerbated a long-term political distrust between the government on one side, and left and libertarian leaning tech workers on the other.

The distrust between the Pentagon and Silicon Valley mirrors the problems that the DoD has faced in broadening its procurement base to civilian-oriented firms. In the case of cyber defense, however, the problem is even more serious; the DoD needs the active cooperation of technology and software firms in order to carry out its cyber security strategy. If private firms are vulnerable to espionage, then the DoD cannot defend its system of procurement or its basic military secrets. There is good reason to believe that hackers in the employ of the Chinese government have worked to exploit this seam.

US–China Cyber Conflict

Experts in the United States began to suspect in the mid-1990s that Chinese hackers were attempting secretly appropriate the technology—one may guess including trade secrets—of American firms working in critical strategic fields through a variety of cyber attacks. Recently, a report from the cyber security firm Mandiant argued that the PLA has played a central role in this process, with what amounts to the official sanction of Chinese government authorities.27 According to Mandiant, a unit associated with the PLA has launched attacks against 141 global firms, many operating in the defense sector.28 Although China is thought to the largest source

28 Ibid., 3.
of attacks, Russia and India are also suspected of appropriating IP.\textsuperscript{29} Reports indicate that these attacks have sought draft patent information, organizational strategy and hierarchy, and trade secrets.\textsuperscript{30}

The data revealed by Edward Snowden and other sources indicates that the United States believes that China has appropriated a considerable amount of technology associated with numerous defense systems, including the F-35 Joint Strike Fighter, the General Atomics MQ-1 Predator drone, and others.\textsuperscript{31} Classified presentation slides published by Der Spiegel indicate the loss of detailed information regarding radar design and engine schematics, as well as “terabytes” of engineering and testing data.\textsuperscript{32} These slides also indicated a US government belief that it had suffered:\textsuperscript{33}

- 30000 incidents
- 1600 computers penetrated
- 60000 user accounts compromised
- $100 to assess damage and repair networks
- 33000 USAF field officer records
- 30000 USN passwords
- Information on
  - Air refueling schedules
  - USTRASCOM (US Transportation Command) Single Mobility System
  - USN Missile and navigation systems
  - USN Nuclear submarine and anti-air missile designs
  - International Traffic and Arms Restrictions (ITAR data)
  - Data on B-2, F-22, F-35, and other systems


\textsuperscript{30} Mandiant, 20.


\textsuperscript{33} Ibid.
The US government has responded to concerns about cyber security by releasing a strategy for digital defense.\textsuperscript{34} Initial steps include creating a watch list for regular cyber offenders and pressuring suspected countries in bilateral fora.\textsuperscript{35} Critics of this approach have called for more robust steps, including support for lawsuits, prosecutions, and visa denials of officials from suspected countries and firms.\textsuperscript{36} At the same time, planners have debated the strategic implications of cyber conflict.\textsuperscript{37} The participation of an active duty PLA unit in efforts to steal US defense sector-related IP indicates that state behavior (in the field of espionage and counterespionage) is adapting to new technological and legal realities. The strategic relevance of cybercrime becomes tied to the rise of IP as a critical national concern.

In May 2014, the US Department of Justice indicted five officers of the PLA on charges of cyber theft.\textsuperscript{38} The US indictment established an important distinction between US espionage policy and Chinese policy. The key difference, according to US policymakers, is that the PLA hackers stole information from private US firms and turned that information over to Chinese state owned firms. US espionage, on the other hand, concentrates on governments and state-owned firms. While the information gained from such espionage may benefit private American firms, it does not involve the straightforward transfer of foreign information to privately owned American companies.

This makes the theft of private, national security-related IP very interesting in context of the development of the modern national innovation system. Virtually every patent owned by traditional national security providers in the United States involves de facto collaboration between the US government and a private actor. Moreover, the steadily expanding involvement of private firms in the defense sector in the United States (and elsewhere) means that cyber attacks on private firms can amount to defense-oriented industrial espionage.

Concerns about the F-35 loom particularly large. The DoD expects the F-35, a product of Lockheed Martin, to fill out the fighter-bomber fleets of not only the US Air Force, US Marine Corps, and US Navy, but also the fleets of nearly a dozen allied states. China could use technical information appropriated from the F-35 project in several ways. First, it could apply technical know-how to efforts to detect and defeat the F-35. This would involve improving the capabilities of Chinese detection and weapons systems in ways that could ensure detection and a successful kill following detection. Potentially, China could share this information with other interested states, just as the United States,

\textsuperscript{35} Nakashima, “U.S. Launches Effort to Stem Trade Secret Theft.”
\textsuperscript{36} Ibid.
Israel, and others shared information about Soviet MiGs with one another during the Cold War. This would fall into a traditional understanding of military espionage and would not represent a significant violation of the IP rights of US firms.

Alternatively, China could use the appropriated technical information to improve its own jet fighters, potentially competing with US aircraft. Some indications suggest that China is moving in precisely this direction. The J-31 fighter prototype, produced by the Chinese military aviation firm Shenyang, reportedly has many features that Shenyang has directly copied from the F-35. The two aircraft are not identical; the J-31 has two engines to the F-35s one, and the J-31 lacks the architecture for VSTOL flight that is central to the F-35. Nevertheless, some similarities suggest that Shenyang had access to proprietary information about the F-35 when designing the J-31.

Adding to the complication, recent reports have indicated that China plans the export of the J-31, and indeed that Shenyang may build the aircraft primarily for the export, rather than the domestic, market. This would put the J-31 into direct competition with the F-35, as the only fifth-generation stealth fighters currently available (the Russian PAK-FA may soon be available to limited customers). Potentially, this could open Shenyang (and the Chinese government) up to legal action under several instruments of international IP law. While it is unlikely that the United States (or any international organization) could enforce a settlement inside China, a ruling could potentially affect Shenyang’s assets abroad.

To be sure, the United States and other countries also engage in cyber espionage, although this espionage generally has different implications for IP law. Reportedly, the US intelligence community (IC) has historically supplied US firms with a variety of intelligence designed to improve their market position and negotiation strategies. The IC has also fed intelligence about foreign military equipment into the private sector of the defense industrial base, although it is less clear that this intelligence gathering has directly affected the ability of US firms to compete with foreign products.

---

43 Ibid.
Industrial Espionage and the Chinese MIC

History of the Chinese MIC

A n explanation of how Chinese cyber espionage affects the diffusion of military technology to China, as well as the innovation process within China, can benefit from a discussion of the history and nature of the military-industrial complex of the PRC. In 1949, the Chinese defense industry produced little in the way of sophisticated military technology. World War II and the Chinese Civil War had destroyed much of the urban industrial base, and the Soviets had confiscated much of the industrial equipment the Japanese had brought to Manchuria. The dire economic situation that faced the PRC in the wake of the revolution made for minimal investment in technological development.

As initially established, the Chinese military–industrial complex distinguished between the strategic weapons complex (nuclear weapons and their delivery systems) and the conventional weapons complex. The former would have the latitude to engage in basic research, as well as a degree of protection from the vagaries of Chinese Communist Party (CCP) politics. The latter would concentrate on production, imitation of foreign technology, and incremental improvement. The strategic complex managed to develop nuclear weapons with minimal foreign assistance in conditions of tremendous poverty. The conventional weapons complex produced a huge number of obsolescent planes, tanks, and ships, often a generation behind the industry standard. Both sides relied on state investment in large-scale, state-owned enterprises.

In the late 1990s and 2000s, the CCP pushed a major set of reforms through the defense industry. The largest, most important firms remained state owned, but were forced to reform in order to increase efficiency and responsiveness, and reduce cost. The government tried to create a competitive environment by splitting firms and setting them against one another, and by stepping up purchases from Russia. Reforms to the system of IP law helped incentivize information sharing and an across-the-board regulatory effort helped bring many firms up to international standards.

The innovative capacity of an MIC extends to more than just the military and the defense industry. It also involves the constellation of labs, research facilities, and universities that facilitate innovation in both the civilian and military economies. This system has existed in some form since the Maoist period, but reforms have attempted to make it more competitive, and more receptive to foreign technology (and even foreign capital). These reforms have helped make the current Chinese defense sector more healthy and innovative than ever. Indeed, unlike the MICs of the United States and Europe, the Chinese defense sector has enjoyed consistent increases in procurement funding.

45 Cheung, 1421.
46 Cheung, 390.
This is not to say that the Chinese defense sector is competitive with the most innovative firms in Europe, Japan, and the United States. Most sectors of the defense industry have concentrated on incremental innovations, adapting newly developed and acquired technologies to old platforms in small batch construction. China has most effectively specialized in what scholars describe as “architectural” innovation, innovations that shifts and repurposes existing technologies in new forms, hopefully with emergent qualities. Architectural innovations can reap tremendous rewards in military technology; the world-beating battleship HMS Dreadnought, for example, represented an architectural innovation. Similarly, the Df-21 carrier-killer anti-ship ballistic missile repurposes existing technology in more deadly form.

China has long exported military equipment to the world, but for most of the post-war period this has involved second-rate, low-technology weapons. The increasing sophistication of the Chinese MIC could make it more competitive for higher tech equipment, but China has had trouble breaking into some of the more lucrative markets. China may be on the verge of some success with the JF-17 fighter, although as this aircraft strongly resembles an updated MiG-21, it does not serve to demonstrate cutting edge technological innovation. Thus far the only customer is Pakistan, but rumors suggest that Nigeria, Egypt, and Argentina may all have some interest.

Public-Private

Historically, China’s defense-industrial base (like its Soviet model) relied on large, state-owned industry to shoulder the burden of innovation and production. The Soviet industrial system tends to support incremental innovation, but struggles to develop new, novel technology. Both the Chinese and the Soviets before them have relied on injections of foreign technology, either through espionage or purchase, to invigorate their defense industries.

The reforms of the 1980s and 1990s pushed the defense industry into the civilian economy, often unwillingly. Firms often had to restructure in order to produce goods for the civilian market, which sometimes reduced efficiency and innovative capacity. However, this restructuring also tended to improve the internal operation of firms, familiarizing them with the prospects of the civilian market.

More recently, the Chinese defense industry has moved toward the Western model, with strong ties developing between large, state-owned defense enterprises and smaller technology firms. In the Chinese case, the lack of access of traditional defense providers to the wider world of military technology (a leftover from 1990s era sanctions resulting from the Tiananmen Square massacre) make it even more important for Chinese defense firms to work with their civilian counterparts.

---


49 Ibid., 2147.
Industrial Espionage

How much does the Chinese MIC depend on foreign technology? Opinions differ, but most analysts say “a lot.” Just on the aerospace side, the influence of foreign technology is clear. The J-10 was based on the IAI Lavi and the General Dynamics F-16; the J-11 is a clone of the Su-27; the JF-17 is a modern development of the MiG-21; and finally, the J-31 is widely reputed to rely heavily on technology associated with the Lockheed Martin F-35.50

China acquires foreign technology through various means, both above and below board.51 On the private side, Chinese firms operating abroad, and in partnership with foreign firms domestically, have access to an array of foreign technologies and production methods. Chinese students study in Europe, Australia, and the United States, becoming familiar with techniques developed in the world’s most advanced research universities. China also acquires weapons and technology transfers through legitimate purchase.

However, we do not yet have a sense of how stolen IP finds its way into the Chinese MIC. Industrial espionage sounds intriguing, but there are many practical obstacles to the successful theft of technology.52 Individual bits of data, even sophisticated data associated with patents and trade secrets, mean little out of context. Would-be thieves need to know a lot about their target, as well as a great deal about the subject matter involved.

In order to produce useful innovation, the cyber soldiers of the PLA need to know where to direct their efforts, and what they need to look for.53 This requires close collaboration between the MIC (which knows what it needs) and the cyber teams (which know where to look). We don’t know how responsive the PLA is to requests for information from the MIC, or from private industry. We also don’t know how stolen information finds its way into the MIC, either on the public or the private side.

Thus far, we have considerable evidence that the PLA steals military-oriented technology from the United States and Europe, and some evidence that it has successfully put this technology to use. During a recent military parade marking the 70th anniversary of the defeat of Japan, the Voice of America listed the foreign-sourced equipment participating in the demonstration, including the HQ-6A surface-to-air missile battery (appropriated from Italy), the J-15 carrier-based fighter, and several other pieces of equipment.54 In most cases, however, the fruits of espionage come in subsystems, rather than in complete weapons.

53 Roper, 103.
Most of the successful Chinese projects have required either significant production data (as was the case with the J-10) or the acquisition of export models (the Su-27). As Chinese products have grown in sophistication, they have begun to compete with targeted systems. The most obvious competition has come from efforts to export the J-11 Flanker clone, but China’s air defense systems have also sparked some interest around the world. The export of stolen technology, however, would open Chinese firms up to an array of potential legal challenges from Russian and Western firms.

China suffers from an additional problem, as its defense industries remain cut off from much of the global arms market. This limits the access of Chinese defense firms to the latest products, technologies, and manufacturing systems. Chinese firms still have some access to the Russian defense industry, but Russia has limited access after a series of controversies over stolen technology, and in any case the Chinese have learned most of what they can from the Russians.

Conclusions

The expansion of IP law, as with many technological and legal developments, has the potential to create contradictory effects on international espionage. On the one hand, the accumulation of data, ease of cyber access, and proliferation of actors makes it easier for hackers and spies to acquire IP. On the other hand, the growing acceptance of international IP law may offer victims a new set of instruments for fighting espionage.

As Susan Sell has argued, international IP protection is, in and of itself, a power play on the part of major economic actors. The construction and maintenance of the rule systems owes itself to the entrepreneurial behavior of private business, working not only through the US government, but also through international institutions. As such, power relations are embedded within the rules of the IP system, and within our entire way of talking about IP. This is one reason why the IP provisions of the Trans-Pacific Partnership have proven so controversial.

But adherence to international institutional frameworks isn’t entirely voluntary. The demands of international organizations (and, in bilateral terms, of the EU and the United States) require the Chinese government to develop a position on IP, a set of policies designed to support that position, and the bureaucracy necessary to execute those policies. While this bureaucracy may lack power initially, over time the state acquires what amount to habits of compliance, where it becomes more problematic to step outside the expectations of the international regime than to stay within them. In China Goes Global, David Shambaugh outlines this process with respect to China’s engagement with the various regimes of the liberal international economic order.

55 Sell, 80.
Thus, the development of a bureaucracy to manage IP rights, which China has begun, almost inevitably produces a policy shift toward compliance. To the extent that the IP regime (in its several institutional faces, including Trade-Related Intellectual Property Rights (TRIPS), the World Trade Organization (WTO), and others) helps form guidelines for appropriate national behavior, the PRC may rein in or otherwise modify the behavior of its military intelligence apparatus.

In any case, a full analysis of the implications of cyber warfare for industrial espionage requires considerably more research. This article hopes to lay the foundation for that research. The future of the Chinese MIC depends, to some extent, on its ability to acquire technology from the United States and elsewhere. The future of US–Chinese relations depends, to some extent, on the size and sophistication of the Chinese MIC.

References


