INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

Risk of State-Sponsored Intellectual Property Theft and Protection

Institute for Homeland Security

Sam Houston State University

Nick Reese and Thomas Morin

Sam Houston State University

Risk of State-Sponsored Intellectual Property Theft and Protection

By Nick Reese and Thomas Morin

Abstract

Intellectual property (IP) is a cornerstone of innovation and economic strength, yet it faces growing threats from state-sponsored theft. This paper explores the significance of IP theft for U.S. national security and economic stability, focusing on the legal frameworks, case studies, and methods used by state actors. It provides actionable recommendations for critical infrastructure owners and advisors to mitigate risks and enhance protections.

About the Authors

	
Nick Reese	**Thomas Morin**
Nick Reese is the founder and CEO of Triantha and a Strategic Advisor to the Space ISAC. He is a former federal government space policy maker and an adjunct professor at the NYU Center for Global Affairs.	Thomas Morin is an Emerging Technology Consultant and curriculum developer at Triantha. He is a graduate of the NYU Center for Global Affairs and is an expert in the geopolitical implications of emerging technology

Authors' Note

The authors would like to thank Sam Houston State University and the Institute for Homeland Security for their support of this important work and dedication to emerging technology education and research for critical infrastructure.

I. Introduction

In December of 2024, Chinese cyber actors made history. Their widespread intrusion into the American telecommunications system made their 2008 attack on the Office of Personnel Management (OPM) look minor in comparison. The attack was notable due to its breadth and that it was executed against critical infrastructure. However, many national security experts had a different take. Many looked at what China did as an indicator of its newfound cyber prowess standing in contrast to some previous attacks that were easily discovered and easily remediated. This time, Chinese actors displayed a level of sophistication that indicates they are no longer the ham-handed cyber actors of old. The Typhoons are getting stronger. China watchers and critical infrastructure personnel should be equally concerned by the Salt Typhoon attack in December 2024, but it would be a mistake to focus only on the tactical aspects of the attack itself. There is another group, a much larger group of people, that should also be concerned.

The U.S. innovation ecosystem is one of the most robust in the world attracting science, technology, engineering, and mathematics (STEM) talent from all over the world. The U.S. has a long history of long research and development (R&D) projects that create technologies that come to market and improve the lives of individuals and the efficiency of organizations across sectors. R&D is vital. It's also slow and expensive. That is why the intellectual property (IP) of companies, universities, and governments is so valuable. Far more than risking a loss of market share, in a geopolitical era dominated by the competition for the research, development, monetization, and operationalization of emerging technologies, IP is strategically important. The ability to shortcut the R&D path and develop a geostrategically important emerging technology could be decisive globally, and that fact is not lost on China nor their cyber actors.

The sophistication of the Salt Typhoon attack should cause concern among critical infrastructure operators but it should also raise flags with companies, universities, and governments who undertake or sponsor technology R&D. The most valuable R&D does not necessarily exist inside a national laboratory or a highly classified defense or intelligence facility. It exists on the laptops of entrepreneurs, students, and engineers for private companies, and those people are targets. The theft of IP presents a direct threat to the economic and homeland security of the U.S. and will, if unchecked, grow into a national security threat. State sponsored IP theft is taking place in the cyber domain as well as the physical domain as the Chinese Ministry of State Security (MSS) is planning and executing intelligence operations inside the U.S. homeland that are directly targeting American citizens and institutions to achieve that edge in emerging technology development. With laws on the books to prosecute and punish IP theft, the U.S. law enforcement community must focus on this compatible issue to mitigate the loss of IP to state sponsored attacks on U.S. soil. As technologies like artificial intelligence (AI), quantum information science (QIS), and space technologies grow to higher levels of maturity, the U.S. must protect its national security and economic assets the way it protects its nuclear arsenal and surrounding technologies.

IP theft is a strategic action intended to give the executing nations a global advantage in emerging technology development, operationalization, and monetization. It also represents a growing issue that crosses the public, private, and academic sectors as well as homeland security and defense authorities. State-sponsored IP theft disrupts this balance by targeting sensitive technologies for geopolitical and economic gains. This paper focuses on U.S. legal frameworks, case studies of state-sponsored theft, and actionable recommendations. Sections include a methodology of research for relevant literature, an analysis of case studies, methods of IP theft, and strategic solutions.

II. Methodology

The research for this paper was conducted through a comprehensive review of relevant and reputable sources, including news outlets known for their investigative reporting on cybersecurity and IP theft, publications from federal (FBI, DHS, etc.) and international government agencies (the EU. etc), as well as peer-reviewed academic articles and research papers. Special attention was also given to relevant laws and regulations like the U.S. Economic Espionage Act, global legal infrastructure like the Trade-Related Aspects of Intellectual Property Rights (TRIPS), as well as other bilateral agreements. These sources were selected to provide a balanced and credible foundation for understanding the scope and methods of state-sponsored intellectual property theft, its impact on industries, and the legal and policy responses addressing the issue. Some priority was given to theoretical perspectives on IP theft as state actors often view IP theft as a strategy to gain economic and military advantages, using it to close technological gaps and assert dominance. Special attention was given to triangulating information across these sources to ensure accuracy and relevance.

III. Methods of Executing IP Theft

States have been attempting to and succeeding at collecting secret information on their adversaries since the beginning of organizational civilization. While the history of espionage is outside the scope of this paper, the dynamic shift between what is considered important enough to steal and the methods by which that information is stolen has shifted recently in ways that should be understood by critical infrastructure personnel, law enforcement, and homeland security professionals across the U.S. This section will examine the methods by which state actors execute their IP theft and will pull from the case studies from the previous section. The intent is to build the foundation for a risk and vulnerabilities framework that can be used by U.S. private sector entities, universities, and critical infrastructure organizations to more effectively plan their defense against IP theft. State actors employ a mix of cyber tools, espionage, and insider recruitment to access IP. Social engineering tactics and academic partnerships often mask their intent. Advanced technologies such as AI and drones facilitate surveillance and data

exfiltration, while joint ventures and research collaborations are leveraged to gain unauthorized access to proprietary knowledge. These coordinated strategies highlight the need for organizations to adopt multifaceted defense mechanisms to safeguard their intellectual property.

Most organizations are aware of the threat posed by cyber threats and many take steps to protect their cyber domain. However, cyber protections are only as useful as the understanding of who is attacking and what they want. Generic cybersecurity practices such as multi-factor authentication, minimum password requirements, file encryption, and firewalls provide a basic level of security for the organization's cyber footprint overall. While these minimum standards are not compulsory outside of a few regulated industries, they remain good practice and should be implemented widely. However, when facing a state-sponsored cyber actor with state-level resources, the minimum cybersecurity practices will not be sufficient to meet the threat. At the same time, not every private sector entity can afford the cybersecurity tools and staff required to run some of the most advanced cyber defenses in places like the federal government or the financial industry. This is what makes the identification of the "crown jewels" so critical. Every organization should understand fully the most valuable information they possess and have an understanding of who might want it and for what purpose. This view on cybersecurity changes the standard view by assuming that a cyber breach may occur, but even in the event of a breach, the most valuable data and/or systems are protected with additional layers.

Cyber espionage has been common for decades, but today's threats include powerful zero day exploits with large teams charged with their deployment and their targets are not limited to other governments. The innovation ecosystem of the U.S. requires a different view of cyber espionage because Chinese actors are not bound by the same restrictions as U.S. intelligence agencies. Next, we will explore the methods by which Chinese actors target private companies for the benefit of their domestic innovation ecosystem in the cyber domain.

Cyber Espionage

Cyber events attributed to China or China-backed actors have been prominent in the cyber landscape since at least 2015 when China hacked the federal Office of Personnel Management (OPM).[1] What has changed is the sophistication and brazen characteristics of Chinese cyber espionage against US targets. In late 2024, US officials announced two hacks attributed to China in the breach of the US telecommunications network[2] and a hack of the US

---

[1] Fruhlinger, Josh; *OPM Hack Explained: Bad Security Practices Meet China's Captain America; 2020;* https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

[2] Lyngaas, Sean; *White House Official: 8 Telecom Providers Hacked by Chinese*: December 4, 2024; https://www.cnn.com/2024/12/04/politics/us-telecom-providers-chinese-hack/index.html

Department of Treasury in December 2024.[3] It will come as a surprise to few readers that China is also willing and able to use this cyber capability against IP theft targets.

The difference between the OPM, Treasury, and telecommunications hacks and hacks against IP targets is one of cybersecurity sophistication on the part of the target. Federal government agencies and critical infrastructure entities are mostly aware that they are targets for cyber events that are backed by nation-state actors with nation-state resources. This is not the "bored teenager in his basement" image that has been popular in years past but an image of teams of individuals working together to create the perfect social engineering, delivery, packaging, and exfiltration scheme around an extremely valuable zero day exploit. Federal agencies have a difficult enough time defending against this kind of concentrated effort. Small technology firms and startups make for easy and attractive targets under this model.

Central to the US's ability to continue to lead in emerging technology development is its ability to help the startup and innovator ecosystems defend their IP from state-sponsored cyber threats. What has traditionally been viewed as a matter for the private sector to deal with, technology IP on a variety of topics such as AI, quantum computing, and space resides with small technology companies. That IP should be considered information with national and homeland security implications and should receive the attention it deserves. The cyber domain is a welcoming one for actors that want to be persistent and enjoy some degree of anonymity. Cyberattacks against organizations with valuable technological IP will not stop so the US must take more seriously the need to protect it.

Non-Traditional Collectors

On June 27, 2017, at the 28th meeting of the Standing Committee of the 12th National People's Congress, a major new law was passed in China. The Chinese National Intelligence Law is a sweeping piece of legislation that gives its intelligence services broad authorities to conduct operations abroad and at home. For the purposes of this paper, Article 7 of the National Intelligence Law is relevant. Article 7 states in full (translation from Brown University):

Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public. The State protects individuals and organizations that support, assist and cooperate with national intelligence work.[4]

---

[3]Tucker, Eric; *Chinese Hackers Accessed Workstations and Documents in a "Major" Cyber Incident, Treasury Says*; December 31, 2024; https://apnews.com/article/china-hacking-treasury-department-8942106afabeac96010057e05c67c9d5

[4]Public Law of the People's Republic of China; *National Intelligence Law of the People's Republic of China*; 2017; https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

This provision means that Chinese citizens, regardless of their employment or direct affiliation with the government, are compelled to participate in intelligence operations in concert with intelligence organizations if they are asked to do so. This is an important provision of the law because it opens the door to the use of non-traditional collectors by opening the field of potential human collectors beyond traditional or known intelligence operators.

Traditionally, intelligence operators arrive in their assigned country posing as diplomats. This is called “official cover” in the business and means that they are under diplomatic protections with an official diplomatic passport. This cover provides a layer of protection for the intelligence professional should they be discovered and possibly arrested for espionage. It also creates confusion among the host law enforcement agencies about who is a real diplomat and who is actually conducting espionage. A common duty among intelligence organizations regardless of national allegiance is trying to identify the intelligence operators of your adversaries. Intelligence organizations go to great lengths to have a picture of who works for an opposing intelligence organization so that surveillance may be put into place should that person or persons ever come to your country. The goal is to know an operative is entering your country before they arrive through the visa or customs processes and to make a decision to put them under surveillance or to refuse them entry.

Non-traditional collectors create a problem with this system. Because of the 2017 National Intelligence Law, the Chinese Ministry of State Security (MSS), the Chinese foreign intelligence organization, is not limited to possibly known intelligence officers. They can choose from a pool of Chinese citizens who may have never had any affiliation with the Chinese government, military, or intelligence apparatus. If that person, perhaps a senior academic researcher, can be trained in basic counter intelligence tactics, they will be extremely difficult for US authorities to identify and track. Intelligence analysts look for connections, even tenuous connections, between potential operators and the Chinese government or the Chinese Communist Party (CCP) to build a case that the individual may be working for the Chinese government. Without any such connection, US authorities have, and will continue to, struggle to identify unaffiliated individuals who have been sent to the US to collect IP under the 2017 National Intelligence Law.

This approach is more effective because even if a non-traditional collector is identified and caught, the penalties have traditionally been light. For example, a non-traditional collector might be charged with lying to a federal official and have their visa cancelled. From the perspective of the MSS, this is a perfectly acceptable risk because the individual in question was never going to be sent back to the US after this operation anyway.

In addition, this approach causes cultural and political tensions as accusations of racial profiling arise.[5] This creates a conflict with the culture of open innovation that sits at the core of many universities and technology companies.

In 2020, FBI Director Christopher Wray called counterintelligence and espionage the "greatest long term threat" to the US economy and called IP theft one of the greatest transfers of wealth in human history.[6] A 2017 estimate put the cost of Chinese IP theft from US sources at between $225 and $600 billion per year.[7] According to the Georgetown Security Studies Review, the FBI opens a new China-related counterintelligence case every 10 hours. This increase represents a 1,300% increase in Chinese economic espionage (IP theft) cases in the last ten years.[8]

The threat posed by IP theft is well documented and not in question. The Chinese government has the domestic tools to execute effective cyber and human-enabled operations that play outside of the boundaries of normal espionage operations. While the US does recognize the problem and has launched initiatives to counter the threat such as the China Initiative and the Disruptive Technologies Strike Force, it is increasingly falling to state and local governments and private and academic organizations to protect themselves from threats. The first step is identification of the problem and education about the scope of the issue. Next, authorities and leaders need to know what to look for and where to look. In the next section, we will cover specific case studies related to IP theft in a university and in the energy sector as a way to illustrate the problem in a real world context.

IV. Case Studies of State-Sponsored IP Theft

IP theft in universities:

State-sponsored actors frequently target universities due to their cutting-edge research, collaborative academic environments and comparatively lax security protocols. Academic partnerships, international student exchanges, and open-access publishing can serve as conduits for unauthorized access to IP. Research in fields such as biotechnology, quantum

---

[5]Financial Times; *America is Struggling to Protect Intellectual Property*; https://www.ft.com/content/1d13ab71-bffd-4d63-a0bf-9e9bdfc33c39

[6] IBID

[7] IBID

[8] Bryja, Tom; *Winning the Race: The Case for Counterintelligence Against Chinese Espionage*; January 17, 2024; https://georgetownsecuritystudiesreview.org/2024/01/17/winning-the-race-the-case-for-counterintelligence-against-chinese-espionage/

computing, and advanced materials is particularly vulnerable. This case underscores the dual challenge of fostering academic collaboration while safeguarding sensitive innovations.

The case of Charles Lieber, former Chair of Harvard University's Chemistry and Chemical Biology Department, underscores the complex risks posed by state-sponsored IP theft in institutions. Lieber was a globally recognized nanoscientist, renowned for his groundbreaking research on nanotechnology, which was heavily funded by U.S. government grants from agencies such as the Department of Defense the National Institutes of Health[9]., However, unbeknownst to his academic peers and federal authorities, Lieber has entered into a secret agreement with China's Wuhan University of Technology (WUT) under the Thousand Talents Program[10], a Chinese government initiative designed to attract top global talent to advance China's technological and economic objectives[11]. While these programs are often framed as legitimate academic collaborations, they have been criticized for their role in facilitating the unauthorised transfer of sensitive technologies. Lieber's case came to light in 2020 as part of the U.S. Department of Justice's (DOJ) China Initiative, which sought to investigate and address state-sponsored economic espionage and illicit academic partnerships[12].

Lieber's involvement with WUT and the Thousand Talents Program was concealed from both Harvard University and U.S. federal grant authorities. Under his contract with WUT, Lieber was paid up to $50,000 per month, received $158,000 annually in living expenses, and was granted $1.5 million to establish a research lab in China[13]. In return, he agreed to publish articles, mentor young researchers, and facilitate collaborations with WUT[14]. Critically, Lieber failed to disclose his participation in this program and the income he received on his tax filings and in federal research funding disclosure-both required by U.S. law. Although the case did not produce direct evidence that Lieber transferred classified information or IP to China, it exemplified how foreign governments use academic partnerships to access advanced knowledge and research conducted in the U.S. Lieber's false statements to federal investigators and failure to report foreign income led to his arrest in January 2020 and his conviction in

---

[9]US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

[10]Federal Bureau of Investigation; *The China Threat*; https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans

[11]United States Senate Permanent Subcommitted on Investigations; *Threat to US Research Enterprise: China's Talent Recruitment Plans*; https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf

[12]US Department of Justice: *Information about the Department of Justice's China Initiative and Compilation of China Related Prosecutions since 2018;* https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related

[13]US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

[14] IBID

December 2021 on charges of making false statements, failing to report foreign bank accounts and tax fraud.

The Lieber case had significant consequences for the academy and national security communities, highlighting the vulnerability of universities to foreign influence and economic espionage. It reinforced the importance of strict compliance with disclosure requirements for federally funded researchers and prompted universities to reexamine their policies on foreign collaborations. In the wake of this case, federal agencies, including the National Institutes of Health (NIH) and the Department of Energy (DOE), issued stronger guidance on disclosure and tightened oversight of foreign research funding. Nevertheless, the case underscored the broader theory of nontraditional collectors, where adversaries use seemingly legitimate avenues like academic partnerships to gain access to sensitive information. The Lieber case remains a cautionary example, driving ongoing debates over how to balance academic openness with national security, particularly as adversarial nations continue to target U.S. institutions to advance their strategic goals. In the wake of the Lieber case, the U.S. government faced criticism over the DOJ's China Initiative, with some arguing that it disproportionately targeted Chinese researchers and collaborators, ultimately ending the initiative[15]. This criticism reflects the challenging nature of the non-traditional collector threat, particularly in the university environment. The vast majority of students in universities are there for legitimate purposes making it difficult and politically treacherous to execute programs to identify and eliminate non-traditional collectors.

Since the Lieber case, China's Thousand Talents program has been widely exposed as a front for IP theft.[16] The exposure has caused Chinese operational planners to shift their tactics to ensure the continued availability of IP. Universities are attractive targets for IP theft given their open learning environments and culture of cross border collaboration. However, many universities hold extremely valuable IP on topics and technologies that are in early stages of development. Such information should be closely guarded by university administrators as a potential national security threat. The Lieber case highlights the need for universities to implement programs that require disclosure of foreign activities to university officials to ensure their IP is safeguarded. Universities should also form close partnerships with state, local, and federal law enforcement agencies to ensure connectivity in the event of an incident. Many university officials are aware of the cybersecurity threats to their data and IP but live human non-traditional collectors are also a threat. Programs to safeguard IP should be built accordingly and not limited to cybersecurity protocols.

---

[15]Lucas, Ryan; *The Justice Department is Ending its Controversial China Initiative*; February 3, 2022; https://www.npr.org/2022/02/23/1082593735/justice-department-china-initiative

[16] Federal Bureau of Investigation; *The China Threat*; https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans

IP theft in the energy industry:

The energy sector, encompassing oil, gas, renewable energy, and grid technologies, is a prime target for state-sponsored IP theft due its role in national security and economic stability. Advanced energy technologies, such as those enabling energy storage or smart grids, can often be the focus of theft, as they provide strategic advantages in both economic and geopolitical contexts. Cyber intrusions, insider threats, and illicit technology transfer through joint ventures are common methods employed to exfiltrate critical energy-sector IP.

The 2014 cyber espionage campaign known as Operation Cloud Hopper was orchestrated by a Chinese state-sponsored hacking group identified as Advanced Persistent Threat 10 (APT10)[17]. This group targeted US companies and several critical industries including the energy sector to steal valuable intellectual property and trade secrets[18]. APT-10's activities were aligned with China's Made in China 2025 initiative which aims to reduce reliance on foreign technologies and establish dominance in key sectors, including energy.[19] The US government has stated that these thefts posed not only economic threats but also risks to national security given the strategic importance of energy infrastructure and technology[20].

APT10 gained unauthorized access to the networks of energy companies by exploiting vulnerabilities in Managed Service Providers (MSPs) - third party information technology (IT) service providers frequently used by corporations to manage their IT infrastructure[21]. The hackers employed spear-phishing emails to trick employees into revealing login credentials, which were then used to breach MSPs and, subsequently, their client's networks[22]. Once inside, the hackers exfiltrated sensitive data, including research on energy systems, proprietary designs, and information on supply chains[23]. Operation Cloud Hopper exemplified how adversaries leveraged cyber espionage to attack energy companies indirectly through the supply chain dependencies

---

[17] Sayegh, Emil. "Spotlight on Apt10." *Forbes*, Forbes Magazine, 22 Feb. 2023, www.forbes.com/sites/emilsayegh/2023/02/21/spotlight-on-apt10/.
[18] IBID
[19]Center for Strategic and International Studies; *Made in China 2025;* June 1, 2015 https://www.csis.org/analysis/made-china-2025
[20] "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.
[21] Sayegh, Emil. "Spotlight on Apt10." *Forbes*, Forbes Magazine, 22 Feb. 2023, www.forbes.com/sites/emilsayegh/2023/02/21/spotlight-on-apt10/.
[22] IBID
[23] IBID

Operation Cloud Hopper had profound consequences for the energy industry and broader US policy. The breach prompted a reevaluation of cybersecurity practices across energy companies in third party providers, with increased focus on supply chain security and stricter compliance requirements[24]. The theft also contributed to deteriorating US-China relations culminating in the 2018 indictment of two Chinese nationals associated with APT10 by the US Department of Justice[25]. Given the nature of this state-sponsored cyber espionage campaign, Operation Cloud Hopper underscores the urgency of international collaboration to combat cyber espionage. The case remains a pivotal example of the intersection between state sponsored cyber crime and economic competition, illustrating the need for robust defensive strategies to protect IP in critical sectors like energy.

IP Theft in Texas:

From 2012 on (with varying levels of activity), the Russian state sponsored cyber espionage group known as Energetic Bear or Dragonfly orchestrated a sophisticated series of attacks targeting energy companies across the United States and Europe[26]. These operations sought to gather intelligence on critical infrastructure and steal proprietary data, posing serious threats to national security and economic stability. Energetic Bear's activities were part of Russia's broader geopolitical strategy to exert influence over global energy markets by undermining competitors and gaining insights into advanced energy technologies[27]. The group's focus on the energy sector highlights the strategic importance of this industry to Russia as many energy exports constitute a significant share of its economy[28]. Notably Texas - a critical hub of the US energy industry - was reported as one of the regions targeted due to its concentration of energy companies and infrastructure[29].

---

[24] Richmond, Nathaniel. "Operation Cloud Hopper Case Study." *SEI Blog*, 4 Mar. 2019, insights.sei.cmu.edu/blog/operation-cloud-hopper-case-study/.

[25] "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[26] Bing, Chris. "The Old Foe, New Attack and Unsolved Mystery in the Recent U.S. Energy Sector Hacking Campaign." *CyberScoop*, 12 July 2017, cyberscoop.com/us-nuclear-hack-russia-energetic-bear-fireeye-phishing-watering-hole/.

[27] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.

[28] Iea. "Russia - Countries & Regions." *IEA*, www.iea.org/countries/russia.

[29] Mara Hvistendahl, Micah Lee. "Russian Hackers Have Been inside Austin City Network for Months." *The Intercept*, 7 Jan. 2021, theintercept.com/2020/12/17/russia-hack-austin-texas/.

Energetic Bear employed a multi-faceted approach to compromise energy companies including fishing emails, watering hole attacks and malware such as Havex[30]. Watering hole attacks involved compromising websites frequently visited by energy sector employees, planting malware to infect visitors' devices. Once inside the network, hackers access sensitive information, including operational data, blueprints for energy infrastructure, and research on industrial control systems (ICS)[31]. The Havex malware was particularly notable for its ability to map and compromise ICS systems, potentially allowing attackers to disrupt operations and connect sabotage[32]. While no confirmed cases of operational disruption occurred, the theft of critical data is significantly increased risk for targeted companies, including those in Texas, where several energy firms were reportedly compromised[33]. The stolen information could have been used to develop competing technologies, compromised systems, or prepare for future attachment energy infrastructure.

The Energetic Bear campaign exposed critical vulnerabilities in the energy sector, particularly concerning supply chain security and Industrial control systems. In Texas, where the energy sector plays a vital role, these attacks highlighted the importance of robust cybersecurity measures to protect critical infrastructure. The US government responded by increasing regulatory requirements and emphasizing the need for public private collaboration on cybersecurity[34]. The attacks also reinforced the theory of cyber enabled economic warfare, which posits that state-sponsored actors use cyber espionage to undermine competitors' economic advantages. Additionally, these events underscored the risks of cascading consequences and interconnected energy networks, as any disruption in Texas - home to extensive oil and gas infrastructure - could have national and even global repercussions[35]. The Energetic Bear case remains a critical example of how state sponsored cyber activities can impact both economic competitiveness and national security.

Analysis of patterns and implications:

---

[30] Rodillas, Del. “Why Havex Is a Game-Changing Threat to Industrial Control Systems – Part 1.” *Unit 42*, 17 July 2014, unit42.paloaltonetworks.com/havex-game-changing-threat-industrial-control-systems-part-1/.

[31] “Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a.

[32] IBID

[33] Symantec. *Dragonfly: Cyberespionage Attacks against Energy Suppliers*,2014, docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers.

[34] “Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a.

[35] “U.S. Energy Information Administration - EIA - Independent Statistics and Analysis.” *EIA*, www.eia.gov/state/analysis.php?sid=TX.

Both universities and the energy sector face distinct but overlapping vulnerabilities. Universities often serve as entry points for initial reconnaissance or data collection, which can later be exploited by malicious actors targeting industry partners. In the energy sector, stolen IP can undermine competitive advantages, compromise infrastructure security, and disrupt innovation. In both cases, the IP theft was sponsored by state actors bringing state-level resources to the operation. Cyber has traditionally been the domain of choice, but increased cybersecurity measures across the sector have given rise to other methods of theft. These trends highlight the need for sector-specific strategies to counteract state-sponsored theft while ensuring operational and research integrity.

In the academic world and in critical infrastructure, growing and maintaining an attractive innovation ecosystem for new technologies is a critical element of continued growth and a way to attract new ideas. If these sectors are unable to protect themselves from state-sponsored IP theft, innovators will not be inclined to build new technologies in these environments. Research and Development is a long and sometimes expensive process, so incentives to shortcut it are high. Competitive advantages will be lost by both academia and industry if this problem is not properly mapped and addressed. The issue becomes one of security of the homeland if it proliferates beyond just a few cases as state actors are conducting sanctioned operations inside the US homeland. The decentralized nature of this problem requires individual organizations to take action commensurate with their mission and priorities. Organizations should prioritize plans for mitigating and reporting IP theft according to the realities on the ground.

Patterns of Theft

Both the Lieber case and the Energetic Bear campaign reveal distinct yet overlapping patterns of intellectual property theft. In the Lieber case, the theft revolved around leveraging academic collaborations to siphon off advanced research, with the Thousand Talents Program acting as a conduit for recruiting US based scientists to share proprietary knowledge[36]. By embedding these relationships in ostensibly legitimate exchanges, the perpetrators exploited transparency norms in academia to mask malicious intent[37]. Energetic Bear, on the other hand, relied on cyber espionage techniques like phishing and watering hole attacks to access sector networks[38].

---

[36] US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

[37] "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases." *Office of Public Affairs | Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases | United States Department of Justice*, 28 Jan. 2020, www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

[38] *Dragonfly: Cyberespionage Attacks against Energy Suppliers*, Symantec, 2014, docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers.

Despite differing operational methods, both cases targeted sectors critical to national security- biotechnology and energy- highlighting a consistent pattern of adversaries focusing on cutting edge technologies and critical infrastructure. These case studies underscore the trend of exploiting systemic vulnerabilities in high-value industries for strategic economic and military gains

Implications

The implications of these thefts extend far beyond financial losses to the victim organizations. The Lieber case demonstrated how state-sponsored programs like the Thousand Talents Program weaponized academic openness to advance technological development in foreign adversary nations, potentially undermining US leadership in key Industries such as nanotechnology. Similarly, Energetic Bear's cyber attacks on the US energy sector revealed the fragility of critical infrastructure, demonstrating how stolen industrial control system (ICS) data could be used for future sabotage or to develop competing technologies. Both incidents underscore the potential for economic espionage to serve as a tool of geopolitical influence, allowing foreign adversaries to accelerate their technological progress while weakening the US's competitive edge and security resilience.

Risk Factors from Case Studies

Key risk factors enabled the success of these thefts in both case studies. In the Lieber case, the decentralized oversight of academic partnerships and inadequate vetting processes allowed the Chinese government to exploit university research programs[39]. Furthermore, Lieber's failure to disclose his affiliations reflected broader systemic gaps in enforcing compliance with federal funding requirements. For Energetic Bear, the risk factors were rooted in the cyber vulnerabilities of the energy sector, particularly its reliance on aging ICS infrastructure and insufficient cyber security defenses[40]. The targeting of Texas-based energy firms, a hub for oil and gas industries, highlights how regional concentrations of high value assets can amplify risk exposure. These cases illustrate how a combination of institutional complacency, lack of oversight and inadequate cybersecurity can create fertile ground for intellectual property theft.

- Decentralized Oversight of Academic Partnerships

[39] "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases." *Office of Public Affairs | Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases | United States Department of Justice*, 28 Jan. 2020, www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

[40] "Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a.

- Inadequate Vetting Processes
- Cyber Vulnerabilities
- Aging Infrastructure
- Insufficient Cyber Defenses
- Lack of Cohesive Strategy
- Lack of Information Sharing

V. Risk Factors and Vulnerabilities for US Businesses

Cybersecurity Defenses in Critical Infrastructure

The case studies of Energetic Bear, the Lieber case, and APT10 illustrate critical risk factors that expose U.S. businesses to IP theft and cyber espionage. One of the most prominent vulnerabilities is the lack of robust cybersecurity defenses in critical infrastructure sectors. Energetic Bear, a Russian state-sponsored threat actor, exploited outdated ICS in the U.S. energy sector, using phishing emails and watering hole attacks to gain access to sensitive operational technology[41]. Many energy firms, those in Texas being no exception, rely on legacy systems that prioritize reliability over security, creating exploitable gaps that allow adversaries to conduct reconnaissance and potentially disrupt operations[42]. Similarly, APT10, a Chinese cyber-espionage group, leveraged weaknesses in managed service providers (MSPs) to infiltrate U.S. corporations, particularly in healthcare, finance, and defense sectors[43]. These cases underscore the growing threat of supply chain vulnerabilities, where businesses unknowingly inherit security risks from third-party service providers.

Exploitation of Academic and Corporate Partnerships

Beyond technical vulnerabilities, the exploitation of academic and corporate partnerships serves as a major risk factor.

---

[41] Bing, Chris. “The Old Foe, New Attack and Unsolved Mystery in the Recent U.S. Energy Sector Hacking Campaign.” *CyberScoop*, 12 July 2017, cyberscoop.com/us-nuclear-hack-russia-energetic-bear-fireeye-phishing-watering-hole/.

[42] “How Renewable Energy Can Make the Power Grid More Reliable and Address Risks to Electricity Infrastructure.” United States Joint Economic Commitee.,19 Jan. 2024, www.jec.senate.gov/public/index.cfm/democrats/2024/1/how-renewable-energy-can-make-the-power-grid-more-reliable-and-address-risks-to-electricity-infrastructure#:~:text=The%20aging%20U.S.%20electrical%20grid,replacing%20in%20the%20coming%20decades.

[43] “Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information.” *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

The Lieber case exemplifies how foreign governments leverage talent recruitment programs, such as China's Thousand Talents Program, to extract cutting-edge research from top U.S. institutions[44]. By providing financial incentives and exploiting weak disclosure requirements, these programs facilitate the illicit transfer of intellectual property, often without immediate detection. APT10 used a different but related tactic—compromising MSPs —to gain access to trade secrets and sensitive research from multiple corporations at once[45]. These cases reveal how businesses and universities, eager to engage in global collaboration, may unintentionally expose proprietary data to foreign adversaries through inadequate oversight and compliance enforcement.

Insider Threats

Another significant risk is the human element and insider threats, which play a crucial role in both cyber and physical theft of intellectual property. While Energetic Bear and APT10 relied on cyber-based intrusions, Lieber's case demonstrated how individual actors within research institutions can become conduits for foreign adversaries. Insider threats—whether intentional, as in Lieber's case, or unintentional, such as employees falling for phishing scams—remain a persistent vulnerability across industries[46]. Many businesses and institutions lack comprehensive security awareness training, making employees susceptible to social engineering tactics that facilitate cyber intrusions. Additionally, the increasing sophistication of state-sponsored cyber operations means that traditional security measures, such as firewalls and endpoint detection, are often insufficient without proactive threat intelligence and real-time monitoring.

This study identified these three major risk factors, which should be operationalized by organizations in the form of a cohesive IP theft risk mitigation strategy and workforce training. These factors serve as a foundation for organizations to build policies and strategies to guide their organizations in the time of increased threat from state-sponsored actors. The threats posed come from both cyber actors and human collectors making risk mitigation difficult. However, organizations can begin mitigating these threats through strategic planning and training their workforce to recognize the threats. The primary recommendations of this paper are:

- Strategic planning to create risk-informed policies

---

[44] US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

[45] "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[46] "Defining Insider Threats: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats.

- Workforce training
- Mapping of the primary targets of IP theft inside Texas

Undertaking these efforts will ensure the integrity of the innovation ecosystem in Texas and beyond facilitating ongoing technological and economic development. IP theft is a threat to organization and to the homeland if left unchecked. It is currently pursued on a small scale by law enforcement necessitating action by individual organizations. This research will help organizations take the first critical steps toward a safe and secure innovation ecosystem.

VI. Recommendations for Critical Infrastructure Owners and Operators

To mitigate the risks posed by state-sponsored IP theft and cyber espionage, critical infrastructure owners and advisors must adopt a multi-layered security approach that integrates both technical and organizational safeguards. One of the most immediate priorities is strengthening cybersecurity defenses through continuous monitoring, threat intelligence sharing, and zero-trust architecture. The Energetic Bear campaign demonstrated how nation-state actors exploit outdated ICS in the energy sector to gain unauthorized access[47]. To counteract this, organizations should implement network segmentation, ensure endpoint detection and response (EDR) capabilities, and regularly update systems to close exploitable security gaps. Additionally, participation in industry-specific cyber intelligence-sharing initiatives, such as the Electricity Information Sharing and Analysis Center (E-ISAC), could enable organizations to stay ahead of evolving threats(*).

Beyond technical controls, enhancing third-party risk management is crucial, as demonstrated by APT10's infiltration of managed service providers (MSPs) to access sensitive corporate and government data[48]. Organizations should conduct rigorous security assessments of all vendors and cloud service providers, requiring compliance with robust cybersecurity frameworks such as the NIST Cybersecurity Framework or the Department of Energy's Cybersecurity Capability Maturity Model (C2M2)(*). Contracts with third-party providers should include strict security requirements, including continuous monitoring, multi-factor authentication, and incident response plans. Furthermore, the push for data sovereignty measures, where

---

[47] "Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.

[48] "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

critical infrastructure companies limit reliance on foreign cloud providers and enforce stronger encryption standards, can significantly reduce exposure to adversarial cyber operations.

Another vital recommendation is strengthening insider threat programs and enforcing stricter disclosure requirements for research and technology partnerships. The Lieber case underscores how foreign adversaries exploit talent recruitment programs to extract sensitive research from U.S. institutions[49]. Critical infrastructure organizations should adopt enhanced vetting procedures for employees and collaborators, particularly those engaged in proprietary research and development. The implementation of continuous monitoring systems for anomalous data access and exfiltration, along with mandatory disclosure of foreign funding for research initiatives, can prevent intellectual property leakage. Furthermore, industry leaders should work closely with academic institutions to ensure that federally funded research remains protected under various regulatory structures.

Understanding where we are most vulnerable is the first step toward effective mitigation. We also recommend that individual organizations create internal maps of where their critical IP resides organizationally and within their virtual environment. To guide this, the State of Texas should create a geographic map of the most vulnerable regions to state-sponsored IP theft and marshal resources to those locations. Creating better security and resilience is always a goal for critical infrastructure and that should extend to IP protection. Understanding the geographic and organizational vulnerabilities is an important step to creating effective risk management.

Lastly, investing in workforce training and incident response readiness is essential to creating a resilient security culture. Employees remain a primary attack vector, whether through phishing attempts, social engineering, or direct recruitment by foreign adversaries. Organizations should conduct regular security awareness training tailored to evolving threats, with a focus on detecting social engineering tactics and recognizing cyber intrusion indicators. Additionally, developing and testing incident response playbooks through red team/blue team exercises ensures that organizations can rapidly contain and mitigate cyber incidents. Close collaboration with government agencies such as CISA, the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), and the FBI's Counterintelligence Division can provide critical infrastructure owners with the necessary support to strengthen their defenses against state-sponsored threats.

By implementing these recommendations, critical infrastructure owners and advisors can build a more secure and resilient operational environment, reducing the likelihood of successful IP theft and cyber espionage campaigns conducted by foreign adversaries.

---

[49] US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

INSTITUTE FOR HOMELAND SECURITY

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water / Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Reese, N., & Morin, T. (2025). Risk of state-sponsored intellectual property theft and protection (Institute for Homeland Security Report No. 2025-1004). Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/E7AD4