# Theft of intellectual property from advanced technology projects[1]

Dr. Robert James Chapman

## Introduction

Today's projects are now almost unrecognisable from projects of 25 years ago. They have benefited from developments in, (for instance): project management methodologies, decision analysis, maturity models, the use of common project management software, taxonomies, work breakdown structures, project controls, risk management, reporting formats, databases, benefits analysis, stakeholder management, optimism bias calculations and use of the internet. While the internet has brought significant and widespread improvements in, for instance, connectivity, communication and the sharing of knowledge, the widespread use of emails, websites and electronic money transfers has exposed businesses to very serious cyber security threats and the potential loss of highly sensitive data.

## Measures of project success

Projects are now facing a tidal wave of cyberattacks and the theft of intellectual property (IP). As a consequence, the measures of success for innovative technology projects (ITPs) undertaken by today's businesses must go beyond the conventional success factors of completing the project deliverables, (within defined cost, time and quality parameters), attaining the identified benefits and satisfying the project sponsor. Given the context of contemporary projects, measures of success must include defending against the theft of IP by cyber security breaches perpetrated by external threat actors (as they are commonly described) or by rogue project team members, (see Figure 1). The technology developed by ITPs is highly prized, given its commercial value. Innovation is occurring in all industries from electric planes and unmanned aerial vehicles (UAVs) to artificial intelligence, facial recognition technology, electric cars, vaccines, medicines, fifth generation mobile networks (5G), renewable energy and space exploration. Typically, businesses developing new technology do not work in isolation but are supported by partners, contractors and suppliers. Each one of these companies present another layer of complexity in that if they suffer a loss of IP by a cybersecurity breach or by a rogue employee, they may in turn compromise (in some cases irreparably) the project they are supporting.

[1] How to cite this article: Chapman, R. J. (2021). "Theft of intellectual property from advanced technology projects"; *PM World Journal*, Vol. X, Issue II, February.

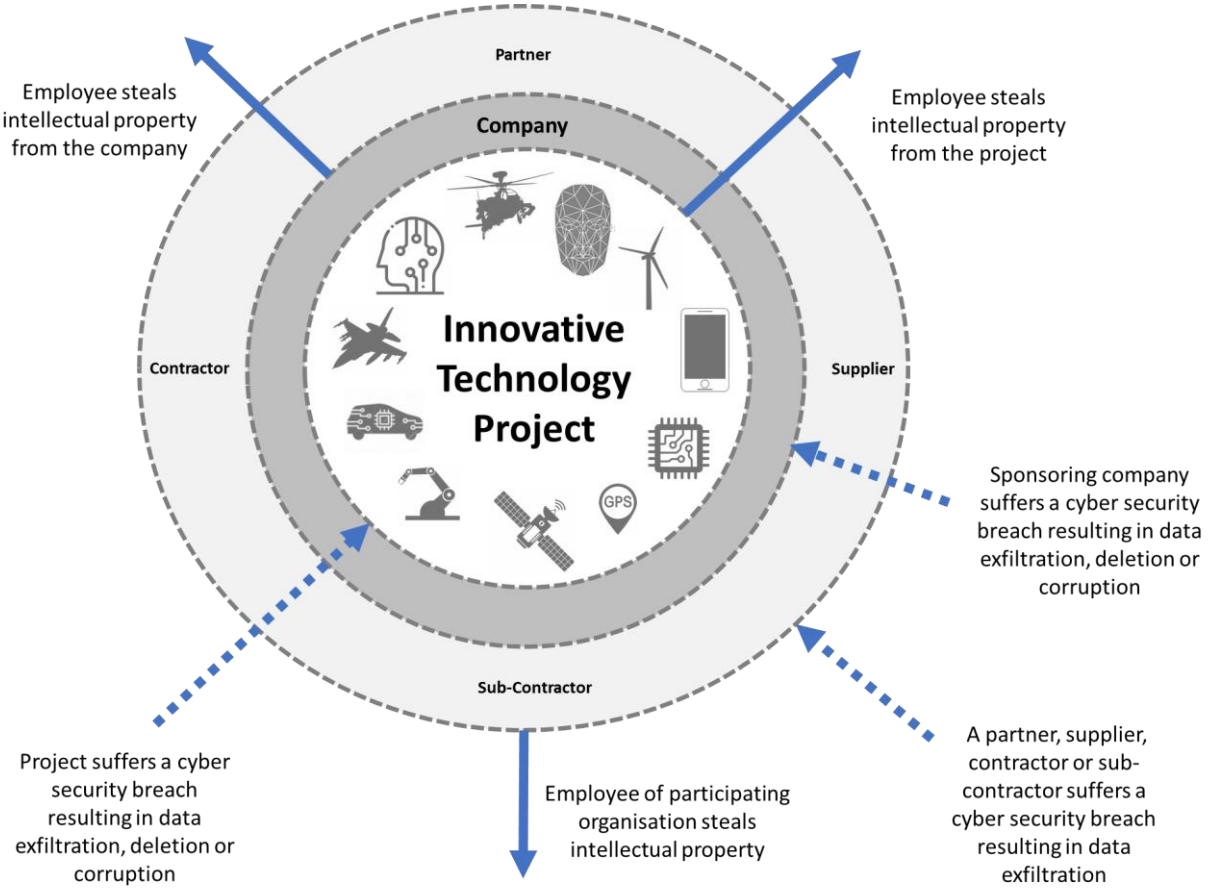


**Figure 1**: Theft of intellectual property by cyber security breaches or rogue employees

## Intellectual property

The definitions of intellectual property and the methods adopted for its protection are common across the developed world. The World Intellectual Property Organization (WIPO) defines IP as creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. Similarly, the U.S. Federal Bureau of Investigation (FBI) defines IP as ideas, inventions, and creative expressions which can include everything from trade secrets and proprietary products and parts to movies, music, and software. Trade secrets are commonly defined as information, (including a formula, pattern, compilation, program, device, method, technique, or process), that derives independent economic value from not being generally known to other persons (and cannot be readily ascertainable by proper means). The UK government defines IP as something that individuals create using their minds. The definition provided by the online Cambridge Dictionary is more expansive and states "IP describes someone's idea, invention, creation, etc., that can be protected by law from being copied by someone else". Likewise, the Canadian government describes IP as including inventions, new technologies, new brands, original software, novel designs and unique processes. In a common vein, the Australian Government defines IP as the property of the mind, proprietary knowledge and the production of new ideas.

## Protection of intellectual property

In the U.S., IP law is governed by both federal and state legislation, as well as being subject to international conventions implemented by WIPO and the World Trade Organization (WTO). The FBI's strategic objective is to detect and disrupt state sponsored groups and international and domestic criminal organizations that manufacture counterfeit and pirated goods or steal, distribute or otherwise profit from the theft of IP. The FBI coordinates with the U.S. Cybersecurity and infrastructure Security Agency (CISA), established in 2018, which builds a national capacity to defend against cyberattacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies. Failure to protect IP undermines confidence in the economy, removes opportunities for growth, erodes the U.S.'s technological advantage, and disrupts fairness and competitiveness in the marketplace. In short, a robust system for protecting IP is critical to economic prosperity. The FBI states it aggressively pursues IP enforcement through traditional investigative methods, intelligence initiatives and coordinated efforts with private industry and domestic and foreign law enforcement partners.

## How is the theft of intellectual perpetrated?

There are a number of situations whereby IP theft may occur, as illustrated in Figure 2. Theft may be committed by what is commonly termed as an 'insider', (an employee), or from outside the business (by external threat actors). Hence it may be perpetrated by a departing company employee with the view to use the IP to start up a new company, take it to a new employer or to sell it (on the assumption a buyer can be found). Alternatively, by an employee who already has links to an organised criminal group, disreputable but legitimate company in the same industry or an aggressive nation state, established prior to joining the business. Externally it may be perpetrated by an opportunist cybercriminal who will initially evaluate the data to understand what will provide the best returns. Options may include blackmailing the owner of the IP or selling it: on the underground economy; to a rival company operating in the same market; or to a nation state. Alternatively, by nation state hackers sponsored by their own foreign intelligence service to steal IP to enable the rapid accumulation of knowledge in the absence of their own country's capability to develop it. Their long-term goal being to make their country technologically and financially superior on the world stage. Other scenarios include a rival company hacker and theft by a competing company which buys the product or article and then reverse-engineers or copies it. The last scenario examined here is theft by a person or persons who physically break into the business premises, a company car or the home of an employee to acquire the information sought.

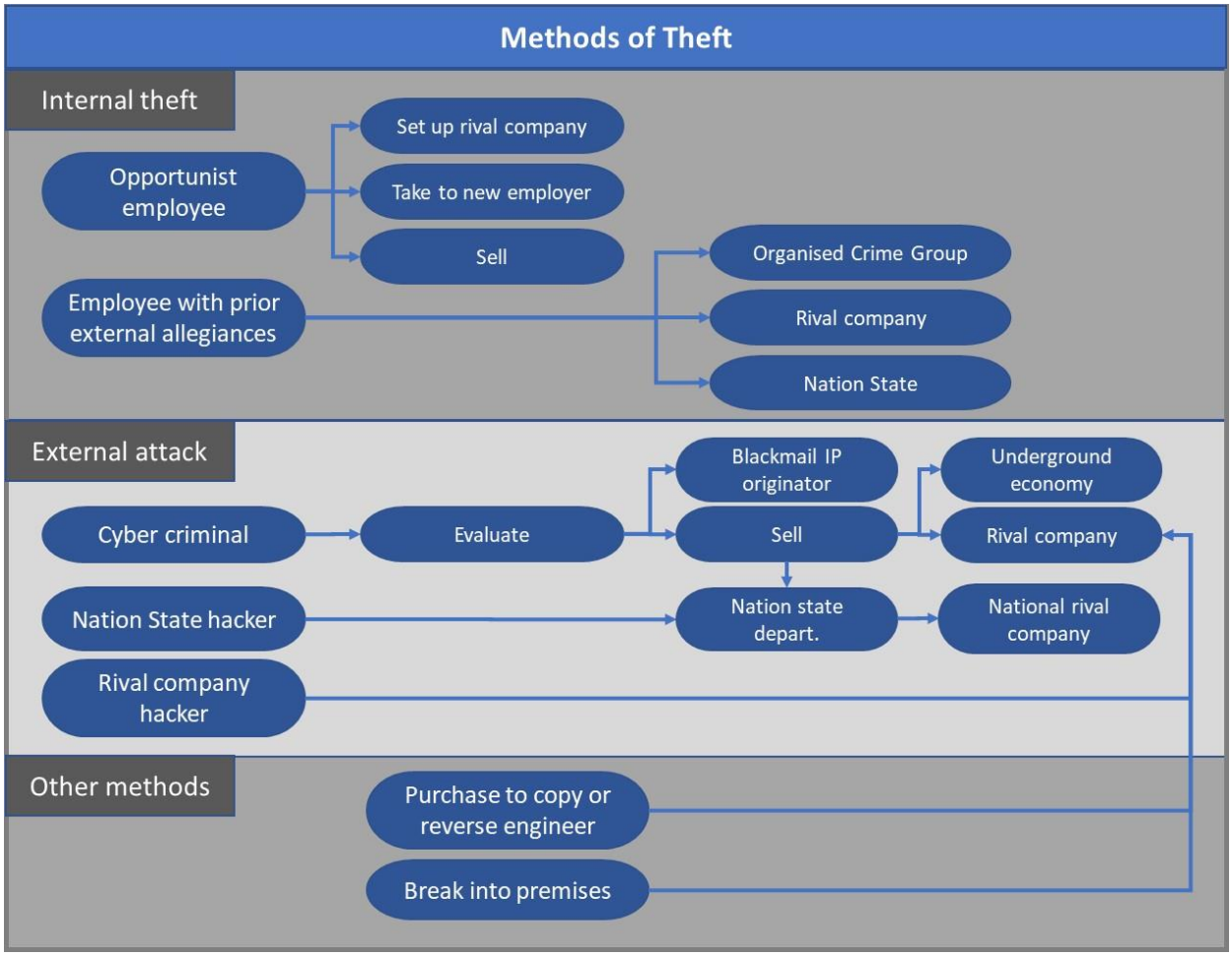


**Figure 2**: Methods of theft of intellectual property

## State sponsored theft of intellectual property

The UK's National Cyber Security Centre has identified the main hostile nation state actors as Russia, North Korea, Iran and China. Global state-sponsored cyberattacks aimed at stealing intellectual property have been highlighted by western intelligence services such as those conducted by Russia's military intelligence service (the GRU), North Korea, formally known as the Democratic People's Republic of Korea (DPRK), the Mabna Institute, an Iran-based company, working on behalf of the Islamic Revolutionary Guard Corps and the Chinese government. Theft of intellectual property by the Chinese government in particular has been prolonged and widespread, with reports of theft spanning back over the last ten years.

China is now the world's second largest economy. Its goal is to be the largest by transforming its position to be the dominant player in advanced technologies. It has adopted a number of techniques to achieve this aim. The Centre for Strategic and International Studies (CSIS) has

been explicit and said China has set out to acquire foreign technology, "either legally or illicitly[2]". This belief is echoed by the Federal Bureau of Investigation (FBI) in its assertion: "China is engaged in a whole-of-state effort to become the world's only superpower by any means necessary"[3]. It expands on this statement by the observation that the "Chinese government is seeking to become the world's greatest superpower through predatory lending and business practices, systematic theft of intellectual property, and brazen cyber intrusions"[4]. During the Hudson Institute video event in 2020[5], FBI Director Christopher Wray identified the Chinese government as one of the greatest long-term threats to the U.S.'s information and IP. The Chinese discovered many years ago that the internet provided them with unparalleled access to poorly secured western computer networks.

The CSIS consider China does not feel constrained by international norms (on trade and investment) or law when it comes to using illegal techniques to gain competitive advantage[6]. In addition, that it has an immense advantage from operating from effectively a closed domestic market and selling to an open international market. Although China is a member of the World Trade Organisation (WTO) it routinely ignores WTO rules[7]. However, to achieve its goals and surpass America, China recognises it needs to make significant advances in today's leading-edge technologies. James Lewis, senior vice president and director of CSIS's Technology Policy Program, has said "China's leaders want to move away from a dependence on foreign technology, so that China moves up the production value chain and is no longer just the assembler of other nations' intellectual property"[8]. The FBI is crystal clear that the Chinese government's ambition is to surpass the U.S.'s economic and technological leadership and to accomplish this, China is acquiring American IP and innovation by any means necessary. Wray identified that the Chinese had pioneered an expansive approach to stealing innovation through a wide range of actors, including not just Chinese intelligence services but also state-owned enterprises, (ostensibly private companies), graduate students, researchers and employees of U.S. companies[9]. He highlighted the targets in the U.S. were both diverse and extensive. Diverse in terms of ranging from Fortune 100 companies to Silicon Valley start-ups and from government and academia to high tech and agriculture. Extensive given that the FBI had ongoing investigations in all of its 56 field offices totalling some 1,000 cases involving China's attempted theft of U.S. based technology, spanning almost every industry and sector.

[2] CSIS (2020) Section 301 investigation. China's acts, policies and practices related to technology transfer, intellectual property and innovation. April 10 2020. Centre for strategic and international studies. https://www.csis.org/analysis/section-301-investigation.
[3] Christopher Wray address at the Hudson Institute, Washington 7 July 2020
[4] FBI ( 2020) The China Treat. 10.7.2020. https://www.fbi.gov/investigate/counterintelligence/the-china-threat
[5] Hudson Institute video event (2020) The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United
[6] CSIS (2020) Section 301 investigation. China's acts, policies and practices related to technology transfer, intellectual property and innovation. April 10 2020. Centre for strategic and international studies. https://www.csis.org/analysis/section-301-investigation.
[7] Ibid
[8] Ibid
[9] Ibid

## Behaviour of an 'organised crime syndicate'

The latest extraordinary behaviour of the Chinese government was reported by FBI Director Christopher Wray at the FBI press conference held on 28 October 2020 at the Department of Justice where he described China's 'Operation Fox Hunt'. The goal of the operation was to harass, stalk, and coerce former Chinese nationals residing in the U.S. to return to the People's Republic of China as part of a global, concerted, repatriation effort. Wray described it as a *"*sweeping bid by General Secretary Xi and the Chinese Communist Party to target Chinese nationals here in the United States and across the world who are viewed as threats to the regime". The targets were political rivals, dissidents, and critics seeking to expose China's extensive human rights violations[10.] The FBI had discovered that family members of Fox Hunt targets who had refused to return to China were threatened and coerced. Those family members living in China had been arrested to apply pressure on their relatives in the U.S. and were used as bargaining chips. One target of the operation (residing in the U.S.) was instructed to promptly return to China or commit suicide. Wray said: *"*These are not the actions we would expect from a responsible nation state. Instead, it's more like something we'd expect from an organized criminal syndicate". In the same press conference Wray went on to say*: "*It's important to understand that Fox Hunt is part of the Chinese government's diverse campaign of theft and malign influence. China is violating laws and norms left and right, from sophisticated cyberattacks targeting our data and personal information, to economic espionage targeting our intellectual property and our trade secrets. And they're using that information to gain influence on the world stage, to gain economic and political power".

## Insider fraud

Insider fraud is conducted by employees of a business or within businesses it is partnering with. Given today's mobility of employees, (particularly recent university graduates and researchers), combined with business's need to attract the most talented individuals to be able to succeed in highly competitive markets, project teams are very often multi-national. Regardless of whether employees have signed contracts containing strict IP and confidentiality clauses (and have agreed to adhere to IP protection procedures), they often believe that the IP they have developed on behalf of their employer should remain in their ownership. Hence departing employees often seek to take with them original project data or copies to their next employer. Insider fraud perpetrated by Chinese nationals has gained overriding prominence due to the frequency and the profile of cases reported in the media and the FBI's repeated assertions over many years of the relentless pursuit of U.S. IP by Chinese individuals. The central Chinese government's Thousand Talents Plan (TTP), re-branded in 2019 as the 'National High-end Foreign Experts Recruitment Plan', sought to entice Chinese scientists to secretly take U.S. knowledge and innovation back to China. In November 2019, the U.S. Senate Permanent Subcommittee on Investigations and the Committee on Homeland Security and Governmental Affairs held an open hearing on the China's Talent Recruitment Plans, including the TTP. The report from the hearing cited numerous cases against TTP members for theft of IP and fraud.

[10] Christopher Wray address at the Hudson Institute, Washington 7 July 2020

## Case studies

Following several prominent cases of attempted or actual theft of IP reported in the media in 2019 (such as those relating to Apple and Tesla), two more recent cases are reported below. American companies that have had their IP stolen by Chinese companies have found the markets they operate in being flooded by cheaper products resulting in a drastic shrinking of their order books and the need to make very extensive redundancies. Theft of IP by Chinese individuals is not confined to the U.S. but has impacted companies across Europe. U.S. businesses need to be alert to the threat and constantly vigilant to protect against IP theft.

**CASE STUDY 1: February 2020**

A U.S. Department of Justice press release[11] dated 27 February 2020 reported that a former associate scientist had been sentenced in federal court for stealing proprietary information worth more than $1 billion from his employer, a U.S. petroleum company. In November 2019 Hongjin Tan, 36, a Chinese national had pleaded guilty to the theft, unauthorized transmission and possession of a trade secret. Tan had been assigned to work in a team with the goal of developing the next generation battery technologies for stationary energy storage, specifically flow batteries. At the hearing Assistant Attorney General for National Security John Demers, said:

> *"This investigation and prosecution uncovered another instance of China's persistent attempt to steal American intellectual property".*

**CASE STUDY 2: July 2020**

A U.S. Department of Justice press release[12] dated 21 July 2020 announced that two Chinese nationals had been charged with hacking into hundreds of victim companies in the United States and abroad. It stated the defendants in some instances acted for their own personal financial gain, and in others for the benefit of the Ministry of State Security or other Chinese government agencies. The theft was prolific running to terabytes of data. The indictment alleged the hackers conducted a campaign lasting more than ten years (up to the present moment), targeting companies in countries with high technology industries, including the United States, Australia, Belgium, Germany, Japan, Lithuania, the Netherlands, Spain, South Korea, Sweden, and the United Kingdom. Targeted industries included, among others, high tech manufacturing; medical devices, civil, and industrial engineering; business, educational, and gaming software; solar

[11] DoJ (2020) Chinese National Sentenced for Stealing Trade Secrets Worth $1 Billion. https://www.justice.gov/opa/pr/chinese-national-sentenced-stealing-trade-secrets-worth-1-billion#:~:text=Thursday,%20February%2027,%202020%20Chinese%20National%20Sentenced%20for,billion%20from%20his%20employer,%20a%20U.S.%20petroleum%20company.

[12] DOJ (2020) "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research". Indictment alleges two hackers worked with the Guangdong State Security Department (GSSD) of the Ministry of State Security (MSS), while also targeting victims worldwide for personal profit.

energy; pharmaceuticals; and defence. At the indictment, Assistant Attorney General for National Security John Demers said:

> *"China has now taken its place, alongside Russia, Iran and North Korea, in that shameful club of nations that provide a safe haven for cyber criminals in exchange for those criminals being 'on call' to work for the benefit of the state, here to feed the Chinese Communist party's insatiable hunger for American and other non-Chinese companies' hard-earned intellectual property, including COVID-19 research,"*

## Summary

At the inception of cutting-edge technology projects, consideration must be given to including within the statement of project objectives, prevention of: the theft of IP by cyber security breaches or the removal or copying of IP data by participating businesses or their employees. In addition, project members should be pressed to strictly adherence to IP protection policies and procedures. Given that innovative projects are often dependent on collaboration between specialist partners, contractors and suppliers – these supporting businesses must take the same precautionary measures against cyber criminals and rogue employees. In addition, because of the behaviour of rogue nation states, employers engaging on advanced technology projects must be on the look out for changes in an employee's behaviour, unexplained absences or foreign trips taken at short notice. For these may be indicators a member of staff is being coerced, blackmailed or encouraged financially to steal intellectual property.

## About the Author

**Robert J. Chapman, PhD**

United Kingdom

**Dr. Robert Chapman** is a Director of Dr Chapman and Associates Limited. He is the author of "Simple Tools and Techniques for Enterprise Risk Management, 2nd Edition", which is recommended reading by the UK's Institute of Risk Management. A discount of 30% can be obtained for the hardback version through the publishers John Wiley and Sons using the promotional code RMD30 and the URL: https://www.wiley.com/en-us/Simple+Tools+and+Techniques+for+Enterprise+Risk+Management %2C+2nd+Edition-p-9781119989974. Select country of residence in the tool bar.

The discount is available from: 2/4/2021 to 2/28/2022

Dr. Chapman can be reached by email at riskappetite@outlook.com