AIR UNIVERSITY | AIR FORCE CYBER COLLEGE

CASE #P03-2109R0
TEACHING NOTES

Hacking the Vaccine

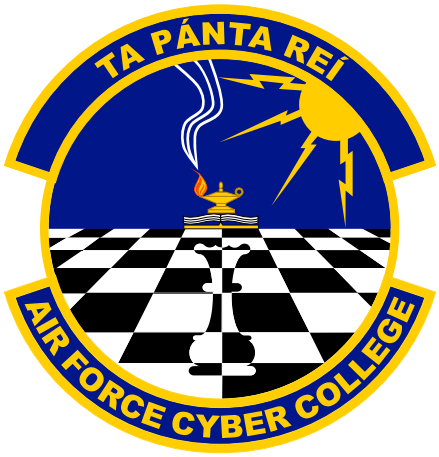
Chad Dacus
Air Force Cyber College

CYBER COLLEGE CASE STUDY SERIES

Air Force Cyber College

Col David B. Bosko, USAF, Commandant

Dr. Karen Guttieri, Academic Dean



Please send inquiries or comments to:

Ms. Kay Adams
Air Force Cyber College
60 W. Shumacher Ave., Bldg 803
Maxwell AFB AL 36112

Tel: (334) 953-5591
E-mail: lillian.adams.1@au.af.edu

Hacking the Vaccine[1]

ABSTRACT

China has long been credibly accused, to the point of criminal indictments, of hacking innovative US firms extensively for the express purpose of industrial espionage. Moreover, obtaining intellectual property (IP) on the cheap appears to be an important element of China's economic strategy. The extent of China's IP theft is impressive, with the US Trade Representative estimating, in 2017, an annual cost between $225 billion and $600 billion. In 2015, the US and China agreed "that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property."[2]

Although it is evident that the agreement initially ushered in some progress, Chinese IP theft continued apace and even extended to life-saving research into developing a COVID-19 vaccine. A vaccine for this deadly virus would save countless lives and be worth billions to its developers. As one would expect, firms and government labs were fiercely competing to make the breakthrough, with more than 90 vaccines being developed as of April 2020—mere months after COVID-19 was identified. On 5 May, 2020, the US and United Kingdom issued an advisory warning of state-sponsored "ongoing cyberattacks against organizations involved in coronavirus response." By 14 May, the Federal Bureau of Investigation (FBI) revealed that it observed Chinese firms "attempting to identify and illicitly obtain valuable intellectual property and public health data" on treating the coronavirus. The Chinese have targeted a wide swath of health care institutions, including pharmaceutical companies, health care bodies, individual academics, medical research organizations, and even local governments.

TARGET AUDIENCE

Graduate students or advanced undergraduates enrolled in cyber law and policy or cyber leadership courses

LEARNING OBJECTIVES

1. Assess the effects of cyber-enabled industrial espionage on US national interests
2. Develop policy options for addressing the current industrial espionage
3. Analyze and recommend policy options for preventing future industrial espionage

---

1. The views presented are those of the speaker or author and do not necessarily represent the views of DOD or its components.
2. Susan V. Lawrence and Wayne M. Morrison, *Chinese President Xi's September 2015 State Visit,* (Washington, DC: Congressional Research Service, 7 October, 2015). https://crsreports.congress.gov/product/pdf/IF/IF10291. This agreement could be a useful avenue of inquiry for possible ambiguity as to the steps China must take.

4. Identify issues in coordinating potentially complex mitigations and responses involving a wide variety of organizations at the national level
5. Distinguish the roles, responsibilities, and authorities of US government (USG) organizations in addressing cyberspace espionage
6. Analyze the relationship of the government with the private sector for addressing intellectual property theft through cyberspace
7. Examine possible benefits and drawbacks of industrial policy (i.e., reasons for the government to interfere in the market)

PURPOSE OF THE CASE

This case deals with the implications of Chinese industrial espionage on US national interests and poses the dilemma of how the United States should respond. As such, many issues may be addressed by the class: from the propagation (and ultimate failure) of cyber norms to the fostering of cybersecurity in private industry.

DISCUSSION

US Government Response

China's history of intellectual property theft plays an important role in this discussion. The Chinese show every indication of continuing their theft. To this point, the US response has largely consisted of "naming and shaming" the Chinese, but the United States and China also agreed to respect the intellectual property rights of others. This agreement led to a temporary pause in theft, but the Chinese are clearly backsliding on the agreement. The US has to decide where to draw the line on non-compliance. The Chinese government shows little effort in cracking down on IP thieves.

1. Does the USG have an obligation to protect all US companies' intellectual property?
   - Does the USG have an obligation to protect US companies who have purposely underinvested in cybersecurity?
   - Does the USG have to protect all companies–large and small?
   - What about other efforts to steal IP that is not COVID-19 related?
   - If at least some companies should be protected, how should the USG prioritize protection of privately-owned assets—for example, critical infrastructure protection?

Beyond the potentially interesting philosophical discussion students might have on this point, they should immediately see that, in a practical sense, what the USG can do for the protection of IP in a $20 trillion economy is necessarily limited. Much of the onus in protecting intellectual property will fall to the research organizations themselves out of necessity. Students should be encouraged to share their thoughts on what the government should or can do to help facilitate their

efforts through information sharing and the provision of tools. Underinvestment in cybersecurity is an important issue, especially for smaller firms who may not be able to afford an acceptable level of investment. An interesting possibility for discussion is what the government can and should do to help smaller firms, in particular. Students should be aware of some of the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA's) programs (found at: https://www.cisa.gov/). Much of the discussion about protecting intellectual property concerning a COVID-19 vaccine can be applied to other industries, but the distinction between the importance of public health IP and other IP could be a useful discussion topic. This distinction led to the identification of critical infrastructure industries and unique security programs for these sectors. More information can be found at https://www.cisa.gov/ics.

2. Identify efforts that can be initiated to protect valuable IP from prying eyes. Which individuals and/or organizations should be involved in this effort?

Discussion: Of course, US research organizations should be well aware that this particular intellectual property is highly sought essentially worldwide. The USG should be as specific as possible in the information they share concerning the threat. DHS's CISA will play the lead role in working with private sector and university research organizations through the National Cybersecurity and Communications Integration Center (NCCIC). Since the intrusion targets will likely be cutting-edge firms and universities, they are likely to have an existing cybersecurity program and processes. As such, their particular interest will be in receiving threat information, and the NCCIC can use this as an opportunity to inform potential participants of the benefits of joining their programs. If the concern is not discussed by students, the instructor can mention that trust could be an issue with private-sector cooperation in any information sharing program. The instructor could mention the Clipper Chip (chipset with a built-in backdoor for law enforcement) as an example of mistrust of government initiatives.[3]

3. Should efforts go beyond protection to law enforcement and/or national security measures?
   - What measures are most appropriate?
   - What are the important considerations in considering what actions to take?
   - Which individuals and/or organizations would be involved?

Students should realize IP theft is a federal criminal offense under 18 US Code § 1831-1839 and opens the door for prosecution for conspiracy to commit computer fraud and abuse under 18 US Code § 1030. In some cases, federal identity theft provisions may have been violated and can be prosecuted under 18 US Code § 1028. Penalties range from 2-15 years. Chinese hackers have

3. Levy, Stephen. "Battle of the Clipper Chip." *The New York Times Magazine*," 12 June 1994. https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.

already been prosecuted using these statutes.[4] Cyber law courses and courses emphasizing legal applications should emphasize the application of these statutes. Prosecuting foreign nationals from a country such as China is particularly problematic since these individuals will almost certainly not be extradited, so some discussion of the practical importance (or lack thereof) of these indictments could be useful. On the national security front, instructors should mention the role of the National Security Agency and US Cyber Command in intelligence sharing and possible counterattacks to possibly deter the Chinese (especially since the United States specifically named Chinese state-sponsored hackers) from continuing IP theft operations. Students may not be as aware of the military's possible role and capabilities, so the instructor should ensure this topic is broached. Chapter 8 of Martin Libicki's *Cyberspace in Peace and War*, which is listed in the references, is particularly helpful on this topic.

4. Does the fact that the vaccine is of paramount importance from a world-wide public health perspective change anything about how the USG should respond?

This can be used as a logical follow-on to question 3. This is more of a philosophical question, and, while an interesting topic for student discussion, can derail the class by taking up all available time. Instructors should be aware of this possibility and plan accordingly. Students should recognize that sharing of intellectual property is antithetical to capitalism but may be warranted when millions of lives might be at stake. Moreover, if IP is to be shared openly, the motivation for corporate innovation evaporates, and the question of how to provide incentives for the effort beyond the market becomes a crucial one to answer. In courses for policy and business students, this issue illustrates some of the tradeoffs involved in socializing medicine. Expanded lesson time could be committed to this particular question depending on the focus of the course.

5. What other factors in the US-China relationship may come to bear in formulating a response—trade negotiations, South China Sea, etc.?

Leadership Challenges

Instructors should ensure that discussion of the potentially complex leadership challenges involved in this case takes place and is not crowded out completely by the more obvious issues surrounding US-China relations. Even an inarguably mild response of targeted measures to improve cybersecurity at the affected organizations would involve leading an effort that heavily involves the private

3. See Department of Justice, Office of Public Affairs. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." Department of Justice website, 19 May 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

sector. These issues apply far beyond this case and are central to the much larger effort of improving cybersecurity in the United States.

6. What are some of the leadership and strategic challenges in potentially implementing recommendations across the whole of government?
    - How do these challenges change at various levels of leadership?

The extent of discussion of leadership issues depends on the nature of the course. Since multiple executive branch departments could be involved in the response, most notably DHS and the Department of Health and Human Services (HHS), students could discuss challenges of collaborating across agencies. For courses with significant emphasis on leadership, Russell Linden's *Leading Across Boundaries: Creating Collaborative Agencies in a Networked World* (complete listing in references) might prove to be a useful resource. Building relationships, effective collaborative processes, and transparency are essential paths to effective multi-agency coordination. Specific to this case, leveraging the existing relationships HHS has built with the affected private-sector entities and transferring some of that trust to DHS would be quite helpful. At lower levels of leadership, general relationship-building and collaboration skills become more important. Again, depending on the nature of the course, legal authorities that constrain action could be a ripe area for discussion. This discussion could eliminate obviously unsupportable approaches that do not envision these constraints. Readings such as Terry R. Bacon's *What People Want: A Manager's Guide to Building Relationships That Work* and Eric Coryell's *Revolutionize Teamwork: How to Create and Lead Accountable Teams* could be useful resources for students and could be incorporated into the discussion.

7. What are some of the leadership challenges in potentially implementing recommendations where private-sector participation is absolutely necessary?
    - How do these challenges change at various levels of leadership?
    - Are incentives necessary here, and if so, what mechanisms might be particularly effective?

This leadership problem is even more challenging. Relationships continue to be important, but the private sector may make for a more difficult partnership, because incentives are not always clear. Information sharing is a particularly vivid example of difficulties that can arise. Corporations are reluctant to share information because this can dissipate competitive advantage and/or cause embarrassment and, therefore, loss of reputation. To overcome these objections, the federal government can anonymize and aggregate information whenever possible, and it can sometimes keep the information confidential to build trust. As previously discussed, potential private-sector mistrust of government participation could be highlighted. Aggarwal and Reddie's "Comparative industrial policy and cybersecurity: the US case" discusses misalignment

of cyber incentives in greater detail than is possible here and is listed in the reference section.

References *(Optional for courses with a focus on leadership)*

Linden, Russell. *Leading Across Boundaries: Creating Collaborative Agencies in a Networked World*. San Francisco, CA: John Wiley & Sons, 2010.

Bacon, Terry R. *What People Want: A Manager's Guide to Building Relationships that Work*. Mountain View, CA: Davies-Black Publishing, 2006.

Coryell, Eric. *Revolutionize Teamwork: How to Create and Lead Accountable Teams*. Naperville, IL: Simple Truths, 2019.

Aggarwal, Vinod and Andrew Reddie. "Comparative Industrial Policy and Cybersecurity: the US Case," *Journal of Cyber Policy* 3, no. 3, (December 2018): 445-466.

US-China Relations Issues

Placing the case in the wider context of US-China relations is paramount. The sheer volume of bilateral trade between the countries provides ample reason to be cautious in response, but the unwillingness of the Chinese to cease their efforts cannot be ignored. So the question could boil down to whether internal measures to protect data should largely be the extent of the US response.

8. In light of the previous agreement on IP theft, should these highly visible attempts to steal vaccine-related intellectual property cause the US to alter its trade policies with China?

China has been credited with making progress in cracking down on IP theft.[5] However, reviews are decidedly mixed on whether there is any real progress.[6] This extremely high-profile violation of the US-China agreement on the protection of intellectual property rights could cause relations to deteriorate further and send the two countries back to square one on the issue. The instructor should focus on playing devil's advocate for the dominant position held by the class.

9. Does China's distinction as the virus's point of origin affect your analysis?

Although this question offers the opportunity for some interesting classroom conversation, the instructor must be careful that this discussion does not devolve into in depth discussions of conspiracy theories. The Chinese disinformation campaign can also sidetrack the conversation if allowed to do

4. See Yukon Huang and Jeremy Smith, "China's Record on Intellectual Property Rights is Getting Better and Better," *Foreign Policy,* 16 October 2019, https://foreignpolicy.com/2019/10/16/china-intellectual-property-theft-progress.
5. See Nicholas Eftimiades, "The Impact of Chinese Espionage on the United States," *The Diplomat,* 4 December 2018, https://thediplomat.com/2018/12/the-impact-of-chinese-espionage-on-the-united-states.

so. The instructor should make sure these conversations tie back to big-picture issues in US-China relations.

10. What can be done to improve China's treatment of intellectual property rights writ large?
    - In light of the long-term nature of this problem, should any recommended response(s) be reconsidered as to how they fit a longer-term strategy of bringing China's policy more in line with what is desired?
    - If China's treatment of intellectual property does not change, what are the long-term implications with respect to US national interests?

Although IP theft involving the Coronavirus is important in itself, students will benefit by putting this episode in the larger context of US-China relations. Since China currently generates a substantial number of patents, and this trajectory will probably continue, it is fairly likely that the Chinese position on this issue will become more favorable in the future. The question may be how to get them to the desired policy state more quickly. Working against this trend is the Chinese culture and the long-held value that both creative and non-creative works belong to the people. Indeed, this belief seems to conform with a collectivist culture writ large. These countervailing forces make this a very challenging question, but the instructor can help steer the conversation to what kinds of policies have the potential to help. Undermining the Chinese Communist Party and its leadership may help, but, ideally, it seems the People's Republic of China (PRC) leadership should be coopted to slowly change cultural beliefs. Visa restrictions (to include drastic reductions in or elimination of student visas), limitation of foreign investment in PRC companies, and exerting pressure on allies to impose similar sanctions are just a few possible policy actions. Instructors should give students license to be creative.

TEACHING STRATEGIES

Depending on the class learning outcomes, the student briefing can focus on a single issue. To stimulate class discussion, students could be assigned a particular issue or issues. Students assigned each question could be responsible for presenting a short PowerPoint briefing and then leading class discussion on that particular issue. The policy options white paper would consist of a more formal discussion of the issue replete with sourcing. Assigning a white paper will dictate careful consideration by the instructor. In most cases, even a five-page paper will only allow for a somewhat superficial analysis since these issues are complex and involve numerous tradeoffs. However, instructors could assign a five-page (or shorter) paper that identifies and briefly explores the important concerns and tradeoffs involved with each issue along with a brief description of avenues for further investigation. Some issues are more amenable to a discussion of policy options, so the instructor may decide to assign those issues to all students for the white paper and separate that assignment from the briefing.

Instructors should consider using a collaborative learning tool such as think-pair-share. Students could be told to think about the issues. Then, depending on class size, students could be split up into groups of three or four. Students within the groups could play specialized roles (some hypothetical roles could be: Assistant to the President for Economic Policy, CISA representative, law enforcement representative, Department of Defense representative, etc.). Alternatively, especially for smaller classes, students could be paired and play multiple roles. Students could be assigned to these roles before class and directed to specific resources to prepare for their roles.

Participants assigned the role of **Assistant to the President for Economic Policy** could focus his or her readings on the Intellectual Property Commission report listed earlier. This role could focus on whether to recommend trade sanctions depending on the magnitude and trends in IP theft. This could lead to an interesting dialogue on targeted versus broad sanctions and the tradeoffs involved.

Those assigned to play the **DHS CISA representative** might identify public-private partnerships to strengthen and possible avenues for new partnerships. CISA's role as lead agency and Sector-Specific Agency for many critical infrastructure sectors should be examined closely by this student or group of students. Those playing this role could be assigned *The Role of Intellectual Property in U.S. Homeland Security* by RAND Corporation.[7]

The **law enforcement representative** should focus on the punishment of cyber crime for both residents and non-residents of the United States. The burden of proof, as contrasted with political attribution, should be a keen focus area. Potential readings are too numerous to list, but a useful resource for identifying indictments and further investigation of these cases can be found in the Department of Homeland Security's *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar*.[8]

The **Department of Defense representative** could focus attention on national security implications of intellectual property theft in this particular case and in general. Debora Halbert's article "Intellectual Property Theft and National Security: Agendas and Assumptions" identifies many of the issues involved.[9]

At the end of class, student groups could then be expected to brief their policy recommendations (to include progression elements) with the class and instructor serving as the National Security Council.

6. Geoffrey McGovern, Maria McCollester, Douglas Ligor, Sheng Tao Li, Douglas Yeung, and Laura Kupe. *The Role of Intellectual Property in Homeland Security.* Homeland Security Operational Analysis Center, 2019, https://www.rand.org/content/dam/rand/pubs/ research_reports/RR3000/RR3039/RAND_RR3039.pdf.
7. *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar*, Department of Homeland Security: 2019 Public-Private Analytic Exchange Program, https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf.
8. Debora Halbert, "Intellectual Property Theft and National Security: Agendas and Assumptions," *The Information Society* 32, no. 4, (2016): 256-268, https://www.ipeg.com/wp-content/uploads/2019/04/Intellectual-property-theft-and-national-security-Agendas-and-assumptions_Halbert.pdf.

CASE PROGRESSION

The following progressions can be added to the case to extend learning opportunities based on available time.

The FBI has determined that Chinese hackers were successful in stealing valuable intellectual property concerning a potential Coronavirus vaccine. Chinese pharmaceutical companies are using the purloined information in their primary vaccine development efforts. Depending on available time, the students could be given a relatively short window to use the same process to update their briefings and present to the class. Instructors can help shape feedback according to other course content and objectives.

Using the stolen intellectual property, the Chinese have developed a competing vaccine and are selling it worldwide at a substantial discount to US developers. Depending on available time, the students could be given a relatively short window to use the same process to update their briefings and present to the class.

Please send inquiries or comments to:

Ms. Kay Adams
Air Force Cyber College
60 W. Shumacher Ave., Bldg 803
Maxwell AFB AL 36112

Tel: (334) 953-5591
E-mail: lillian.adams.1@au.af.edu