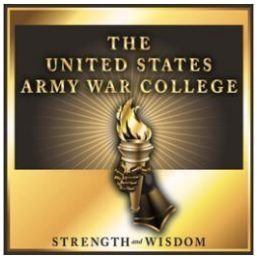
Strategy Research Project

Protecting Virtual Intellectual Property

by

Lieutenant Colonel John F. Cadran
United States Army Reserves

Under the Direction of:
Colonel Scott E. Sanborn



United States Army War College
Class of 2017

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2017	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Protecting Virtual Intellectual Property

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel John F. Cadran
United States Army Reserves

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Scott E. Sanborn

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A: Approved for Public Release. Distribution is Unlimited.
To the best of my knowledge this SRP accurately depicts USG and/or DoD policy & contains no classified information or aggregation of information that poses an operations security risk. **Author:** X **Mentor:** X

13. SUPPLEMENTARY NOTES
Word Count: 5,752

14. ABSTRACT
The theft of intellectual property (IP) threatens the United States' economy and national security. This unparalleled theft of IP is damaging our economy and its current trajectory threatens the future economic security of the United States. This paper examines IP theft by first taking a historical look at economic espionage. This paper then highlights the stark inability to deter IP theft in the cyber domain because of the fundamental differences between virtual IP and physical IP. After which, this paper analyzes current efforts to deter IP theft and shape international cyber behavioral norms. Finally, the paper offers two recommendations in order to counter this risk to national economic security. First, the U.S. must increase funding for the Department of Justice to help deter future theft and reinforce emerging international cyber behavioral norms. Additionally, the Department of Homeland Security (DHS) must mandate a data exchange standard so that cyber threat information can be exchanged and acted on in near-real time.

15. SUBJECT TERMS
Cyber, Cyberspace, Cyber-Enabled Theft

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	28	

Protecting Virtual Intellectual Property

(5,752 words)

Abstract

The theft of intellectual property (IP) threatens the United States' economy and national security. This unparalleled theft of IP is damaging our economy and its current trajectory threatens the future economic security of the United States. This paper examines IP theft by first taking a historical look at economic espionage. This paper then highlights the stark inability to deter IP theft in the cyber domain because of the fundamental differences between virtual IP and physical IP. After which, this paper analyzes current efforts to deter IP theft and shape international cyber behavioral norms. Finally, the paper offers two recommendations in order to counter this risk to national economic security. First, the U.S. must increase funding for the Department of Justice to help deter future theft and reinforce emerging international cyber behavioral norms. Additionally, the Department of Homeland Security (DHS) must mandate a data exchange standard so that cyber threat information can be exchanged and acted on in near-real time.

Protecting Virtual Intellectual Property

> The cyber-enabled theft of U.S. intellectual property is the "greatest transfer of wealth in history."
>
> —General Keith Alexander,
> Director, Nation Security Agency[1]

The theft of intellectual property (IP) threatens the United States' economy and national security. The scope and magnitude of this theft is greatly enabled by cyber espionage. Estimates place the economic impact at over 300 billion annually of which China is responsible for roughly 70%.[2] This unparalleled theft of IP is damaging our economy with job losses considered to be over one million.[3] On its current trajectory, the theft of IP threatens the future economic security of the United States by reducing the incentive to innovate and invest in research, development and engineering (RD&E).[4]

This paper examines IP theft by first taking a historical look at economic espionage. This paper then highlights the stark inability to deter IP theft in the cyber domain, which is followed by an analysis of current efforts to deter IP theft and shape international cyber behavioral norms. Finally, the paper offers two recommendations in order to counter this risk to national economic security. First, the U.S. must increase funding for the Department of Justice to help deter future theft and reinforce emerging international cyber behavioral norms. Additionally, the Department of Homeland Security (DHS) must mandate a data exchange standard so that cyber threat information can be exchanged and acted on in near-real time.

Since its founding, the U.S. has been both the benefactor and the victim of IP theft. America's pre-industrial history is storied with men like Samuel Slater and Francis Cabot Lowell, who made their fortunes by stealing textile industry IP and bringing it to America. Slater, considered by historians as the "father of the American industrial

revolution," was born in England in 1768.[5] He grew up working as an apprentice in a textile factory and by the time he reached 21, the United States had a burgeoning textile market.[6] Though great producers of cotton, the U.S. had little ability to process the cotton and the majority of it was shipped to England. Slater recognized the immense economic potential in America and he emigrated to the United States in 1789[7]. He came to America by presenting himself as a farm hand to British customs authorities. This was in clear violation of British export and emigration laws aimed at preventing equipment and individuals with specific manufacturing knowledge from leaving England.[8] Prior to leaving England, he committed textile machine specifications to memory and by 1793 he helped establish the first water-powered roller spinning textile mill in the United States.[9] This act earned him the dubious moniker "Slater the Traitor" by his former countrymen.[10] While Slater may be considered the father of the American industrial revolution, Lowell is credited with expanding on Slater's effort and modernizing America's textile factories.[11]

Lowell, an American, toured textile factories throughout Glasgow and the surrounding areas, 1810 and 1811, to surreptitiously gather as much information as he could with an eye towards improving American textile manufacturing.[12] A Harvard educated mathematician with a keen mind, Lowell was able to commit to memory what he had learned and thus elude British customs when he left in 1811.[13] His efforts proved quite successful and by 1813 he had established a cotton mill in Waltham, Massachusetts.[14] His mill was the first in the U.S. to house the entire production process under one roof. The efforts of Slater and Lowell contributed immensely to the United States becoming one of the world's leading industrial economies by mid-1800s.[15]

Although examples from the past provide corollaries to today's IP theft, they pale in comparison in both magnitude and scope. The global information networks provide opportunities to steal IP at an unprecedented scale and nation state and non-nation state actors participate. And given that American law enforcement rarely prosecutes these crimes, companies are essentially left to fend for themselves.[16] Unfortunately, companies are not able to defend themselves adequately, which in part stems from fundamentally different approaches in how virtual IP is protected as compared to physical IP.

Physical IP exists, as the name implies, in the physical domain and includes such things as blueprints, prototypes, printed reports of proprietary data. These are distinct from virtual IP, which exists only in electronic form, such as software, computer aided design (CAD) diagrams, and proprietary market research data. Of course, virtual IP can be transformed into physical IP, such as by printing the research data. Nonetheless, by distinguishing physical IP from virtual IP, a model emerges that helps illustrate the variance in abilities of companies to protect their intellectual property in cyberspace versus their ability to do so in the physical domain.

Corporations depend on rings of defense to prevent and deter physical IP theft. In order to steal physical IP, an adversary must contend with multiple layers of physical security. Figure 1 demonstrates how the first layer of defense of physical IP starts with the corporation. At this defensive ring, the company protects its information by storing the IP in a container of some sort, such as a safe. This container is typically housed in a building protected by locked doors, protected by security guards and surrounded by a

perimeter fence. The facility may even integrate monitored technical surveillance measures, such as cameras and motion sensors, to provide further protection.

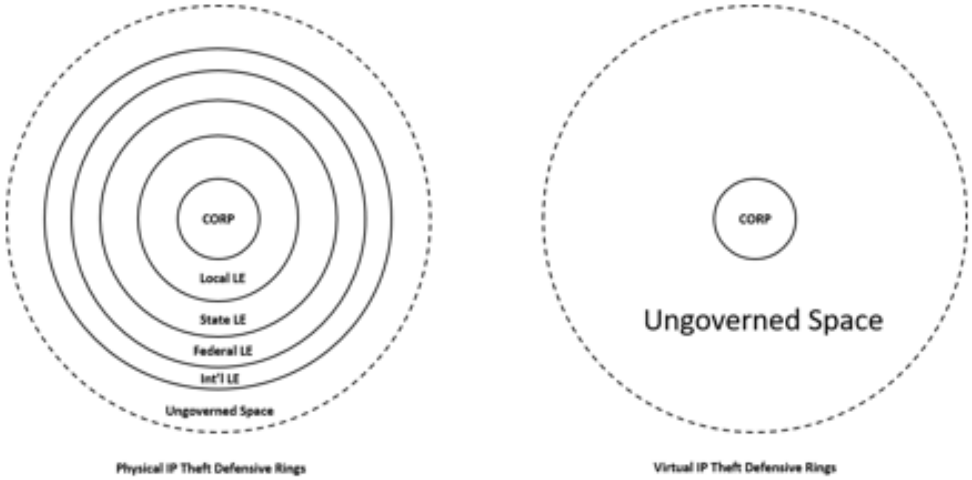


Figure 1. Physical vs. Cyber Rings of Defense

In addition to physical deterrents such as locked containers, doors, and fences, law enforcement also acts as a unique deterrent to prevent physical IP theft. Outside of the building's perimeter, local law enforcement provides visual deterrence by patrolling the area and is available to respond in the event of an incident. These defensive rings ripple outward to the state, federal and international law enforcement communities. Virtual IP has no analogous defensive rings beyond corporation's first layer of defense.

At this inner most layer, the company protects its virtual IP by securely storing it. The virtual IP can be encrypted and access can be limited to a select group of employees. This is analogous to storing physical IP in a safe with a limited number of employees that know the combination. Additionally, firewalls and network intrusion detection devices are, in many respects, similar to locked doors, fences and security cameras. Whereas, network system administrators act as security guards monitoring

the network environment. But it is at this inner most level where the protection similarities end.

Outside of the corporation's defensive rings is ungoverned space. There is no local law enforcement presence outside of the company's network providing "virtual" deterrence. Even if there were such a thing as "virtual deterrence patrols," jurisdictional authority would present significant hurdles to local law enforcement because networks cross city, county, state, and national boundaries. Federal law enforcement could provide some deterrence, but for reason discussed later, their response to virtual IP theft has been limited. However, when physical IP is stolen, law enforcement at all levels is available to respond.

If a suspect is identified, law enforcement from the local to the national level exists in order to apprehend the suspect. Even if the suspect is outside of the U.S., international law, treaties of extradition, and international law enforcement officers can all assist to apprehend the suspect and bring the suspect to justice. These law enforcement actions of patrolling, responding, arresting and prosecuting thieves, deters physical IP theft by shaping and reinforcing accepted behavioral norms but they do not transfer to the deterrence of virtual IP theft.

The reason that deterrence does not transfer to virtual IP theft is rooted in the nature of deterrence and the circular relationship between norms and enforcement of norms. Among legal community scholars, deterrence theory postulates that the greater probability for deterrence is directly related to how "certain, swift, and/or severe" the legal sanctions are perceived.[17] Societal and cultural accepted standards of behavior are expressed through law, whereby law "deters unethical behavior and unethical

behavior is typically illegal."[18] These behavioral norms regulate individual and societal actions and deter the theft of IP. The theft of virtual IP, to date, has certainly not brought swift legal sanctions nor is illegal cyber behavior viewed as entirely unethical as described in the following example.

The theft of music illustrates how law enforcement and behavioral norms differ between the physical domain and cyberspace. An individual that steals a music CD from a store must circumvent numerous security measures such as security cameras, security personnel, and anti-shoplifting security tags. The punishment for shoplifting is well known and society vigorously enforces its condemnation of this behavior. Store security, loss prevention officers, and local law enforcement frequently apprehend shoplifters stealing CDs. On the other hand, those that illegally download music do not have the same security concerns nor are they faced with the same level of enforcement efforts. As a result, the relationship between the law, ethical behavior and illegal downloading is not well defined, which creates the perception that illegally downloading music is "less aberrant than other illegal behaviors."[19]

The reasons for this perception are numerous but the probability of being caught and the belief that no harm is being committed are particularly relevant. One study showed that approximately one-fifth of illegal downloaders of music would steal a CD from a store if they knew they would not be caught.[20] This indicates that for a segment of the illegal downloaders, the risk of being caught plays a role in deterrence. It, therefore, could be extrapolated that an increase in law enforcement arrests and prosecutions for illegal downloading would increase the risk and therefore deter some of

the illegal downloading. This same study also showed that the "no harm, no foul" category of the Consumer Ethics Scale plays a role in justifying the illegal behavior.[21]

The Consumer Ethics Scale, developed by Dr. Muncy and Dr. Vitell, looks at dimensions of consumer beliefs related to questionable behaviors. For example, the scale measures various ethical perceptions of consumers if they were to gain benefit from doing something illegal, or whether no one was harmed by their actions – in essence a victimless crime.[22] The study revealed that music downloaders were less likely to believe their illegal behavior caused harm to either music producers or other consumers.[23] Nor do they believe that digital piracy laws are enforced. As a result of these beliefs, illegal behavior becomes normalized in the cyber domain. Consequently, the lack of legal and societal behavioral norms creates a deterrence vacuum with respect to virtual IP theft.

Nation states and non-state actors exploit this deterrence vacuum and conduct nearly unabated and incessant attempts to steal virtual IP by constantly probing and scanning a company's network from the ungoverned space. A company's network security device may prevent individual network attacks, however, the network device does not deter the malicious actor. Even if an intrusion is prevented by some technical means, network administrators generally do not deter threat actors but only temporarily delay them, while the actors remains free to adapt and try different attack avenues. It is often said in network security circles that there are two types of companies, those that know their network has been compromised, and those that just haven’t discovered it, yet.

If a company discovers its network is compromised, it must then determine if virtual IP was stolen, which can prove quite vexing. Often times, network defenders do not detect the intrusion for months or even years, thus allowing a malicious actor to steal virtual IP over long periods of time. Computer forensic science is still in its infancy when compared to physical forensic science and techniques for discovering theft are limited primarily to analyzing network logs and access logs. However, these logs are voluminous and can require costly storage solutions. As a result, companies often do not store their logs for sufficient periods of time and, therefore, cannot definitively determine what was stolen or how much was stolen. Although determining that virtual IP was stolen is problematic, it is often more difficult for companies to determine who stole their virtual IP.

Attribution remains the most difficult aspect of determining responsibility for virtual IP theft. This difficulty is a function of how computers communicate and who controls the computers and infrastructure. A company can determine which computers from outside its network are communicating with computers inside its network via its server logs. The logs identify who initiated the communications, how long they communicated, as well as the amount of data transferred between computers. This information, though helpful for understanding, is usually insufficient for attribution as we will see in the following example.

Figure 2 illustrates the difficulty in determining the identity of malicious actors in cyberspace, as they go to great lengths to hide their trail and ultimately their location and identity. In this simplified scenario, a malicious actor sends Company X a spearfishing email with a malware attachment. An employee opens the attachment,

which installs malware on a Company X computer. The malware is programmed to communicate with a command and control (C2) server that the malicious actor set up somewhere on the Internet. The malware searches for and retrieves Company X's virtual IP and sends it to the C2 server. The C2 server then forwards the stolen virtual IP to a file storage (FS) server located somewhere else on the Internet. The malicious actor logs into the FS server and retrieves the stolen virtual IP, all the while never revealing his/her location or identity to Company X.

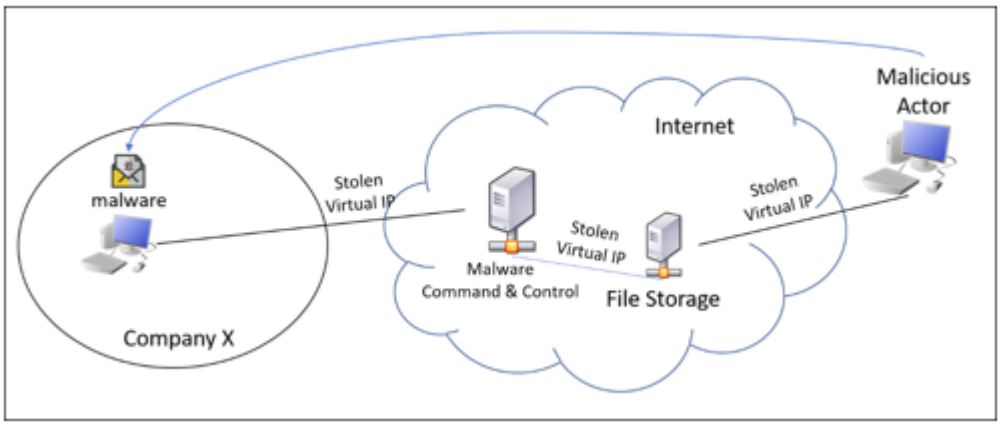


Figure 2. Attribution Difficulties: Inability to Locate and Identify Malicious Actor

The reason the network administrator of Company X is unable to identify the actual malicious actor is a function of what information the logs file collect. As previously described, the network log files contain the forensic evidence of computers in Company X's network that are communicating with other computers However, the only computer that Company X will see in the log files is the C2 server. Because the C2 server is not the final destination of the stolen virtual IP, the network defender needs to know who else is communicating with the C2 in order to determine the identity of the malicious actor, but this will prove difficult.

Company X must request from the owner of the C2 server to view and analyze the logs in order to determine the next step in the trail. Since the owner of C2 server is under no obligation to provide the logs, Company X must ask law enforcement to issue a warrant to compel the owner to provide the logs. If the investigator obtains the C2 server logs and the logs irrefutably show the transfer of stolen virtual IP to the FS server, then the process repeats, requiring an additional warrant to obtain FS server logs. Law enforcement will have a difficult time locating and identifying the malicious actor because the malicious actor could hop across multiple servers from virtually anywhere in the world. Law enforcement will have to coordinate with a foreign government to retrieve the log files if any of the servers or computers are located outside of the U.S. The scope of this simple scenario could easily expand to proportions that would dramatically frustrate most investigations, such as the Chinese advance persistent threat (APT) hackers.

APT is a label given to hackers that maintain unauthorized access to a network, usually with the intention of stealing information. An APT is often associated, resourced or employed by a nation state. The report "APT1: Exposing One of China's Cyber Espionage Units," published in 2013, by the cybersecurity firm Mandiant, provides a particularly stark example of the investigative challenges against an APT.[24] The single malicious actor scenario described above, uses one C2 server, and one victim company. In the Mandiant report, Chinese state sponsored hackers used over 900 C2 servers in 13 different countries in a two-year period.[25] Additionally, the Chinese hackers compromised 141 companies across 20 major industries.[26] Given all of the difficulties with attribution (identifying the real identity and location of the malicious

actor), it should not be a surprise that law enforcement is often unable to protect virtual IP. Not only are there insufficient resources, there are not enough trained law enforcement officers at the federal level to conduct investigations in order to appreciably deter virtual IP theft and shape cyber norms of behavior.

In recognition of a lack of international cyber norms and an inability to significantly deter the theft of virtual IP, the U.S. government is taking a comprehensive approach to this problem. The approach aims to establish and enforce international cyber norms of behavior and better defend cyberspace in order to deter the theft of virtual IP and to better protect virtual IP. In a first step towards establishing and enforcing international cyber norms, the White House published the President's policy for International Strategy for Cyberspace (ISC), in 2011.[27]

The ISC is a strategy designed to establish international cyberspace behavioral norms through policy guidance that establishes the protection of intellectual property as a national priority. The strategy recognizes that the continual and persistent theft of virtual IP by criminals or nation states can result in everything from “unfair competition to the bankrupting of entire firms, and the national impact may be orders of magnitude larger.”[28] The rate of technological change has out-paced states' ability to develop mutually acceptable norms of behavior, which contributes to the perception that cyberspace is the wild west. In order to tame the west, the policy lays out a roadmap that sets priorities to enable USG departments and agencies to plan, coordinate and execute the comprehensive strategy to create a safe and secure cyberspace.[29]

To implement lasting change, the policy commits to establishing international norms of behavior in cyberspace by holding accountable those that violate the norms.[30]

The U.S. demonstrated its resolve to hold nations accountable when the Department of Justice (DOJ) indicted five Chinese military hackers from the Third Department of the Chinese People's Liberation Army (3PLA), in 2014, the same ones identified in Mandiant's APT1 report.[31] The indictment accused the Chinese state actors of stealing virtual IP from companies such as Westinghouse, U.S. Steel, Alcoa, and many others in order to "obtain economic advantage for its state-owned industries."[32] This indictment was the first time in U.S. history that charges for hacking were brought against state actors.[33]

History shows that IP theft has occurred even at the time of this nation's founding but that was primarily individuals or corporations stealing the IP. China's use of state assets to fund, resource and direct the theft of virtual IP violates acceptable norms of nation state behavior. China's state sponsored economic espionage is tantamount to the U.S. government using the resources of the National Security Agency to help U.S. corporations. Take the analogy a step further, in the physical domain, this behavior is comparable to sending the U.S. Special Forces to break into Rolls Royce to steal the plans for the next generation engine so that Ford Motor Company could get an economic advantage. Every nation would recognize this as a violation of sovereignty and intolerable.

Though this physical domain analogy may seem absurd, the sheer volume of virtual IP theft threatened to upset established international economic behavioral norms by undermining the U.S. national economic security. It is even possible to imagine that behavioral norms would be altered to such a degree that states, including the U.S. would engage in economic espionage for survival in a globally connected world.

Another possibility is that the U.S. might respond more forcefully to protect its economic security. The U.S. indictment of five Chinese 3PLA hackers sent notice to nations that the U.S. will not tolerate the use of state resources for commercial and economic gain. At the same time the U.S. also recognizes that charging five Chinese state hackers would not be sufficient in changing all international behavior.

The U.S. realizes that they cannot create international cyber norms alone. As a result, the U.S and China agreed, in 2015, that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." [34] This agreement was monumental for two reasons. First it formally recognized that theft of virtual IP by state governments runs counter to international norms of behavior not just the U.S.'s interests. Second, it established that international behavioral norms in the physical domain also apply to the cyberspace domain. This is particularly noteworthy because prior to making this agreement, China was, according to the U.S. National Counterintelligence Executive, "the world's most active and persistent perpetrators of economic espionage."[35]

By agreeing that state-sponsored cyber-enabled IP theft runs counter to international norms of behavior, China now recognizes that international behavioral norms in the physical domain are applicable to cyberspace. It is also a recognition that bad behavior in cyberspace has real-world consequences. Unfortunately, recognition that the behavioral norms apply to cyberspace is, however, separate and distinct from

compliance and enforcement of these norms. In fact, this agreement may have been simply a politically expedient response to forestall a more dramatic U.S. response.

Amy Chang argues in her article, *Warring State: China's Cybersecurity Strategy* that "China's foreign policy behavior, including its cyber activity, is driven primarily by the domestic political imperative to protect the longevity of the Chinese Communist Party (CCP)."[36] If Chang's assertion is true, then how should the U.S. interpret China's willingness to publicly declare that the Chinese government will no longer conduct or support economic espionage? Is this a recognition that China's leaders no longer see a threat to the CCP or is this a political calculation that the burden of proof for virtual IP theft is so high as to always allow for plausible diplomatic deniability? Or does China simply believe that even if caught, the U.S. will be unwilling to respond forcefully?

Irrespective of China's motive, the agreement may prove extremely difficult to enforce. China was politically and diplomatically embarrassed by the indictment of five 3PLA individuals.[37] Additionally, the Mandiant report outlines exactly how they discovered, tracked and determined that PLA Unit 61398 was behind a large scale, long-term cyber espionage campaign.[38] We, therefore, should be expect that China will improve its operations security by avoiding the methods and indicators documented in the Mandiant report. The tactics and techniques for stealing virtual IP will evolve, which will increase the difficulty in definitively showing that the economic espionage is state sponsored. Consequently, the U.S. government must evolve to keep pace with the threat.

While the U.S. and the international community grapple with compliance and enforcement issues, IP theft continues. The U.S. Trade Representative, “Special 301

Report”, (an annual review of intellectual property rights (IPR) protection and enforcement) still reports China as being the most persistent and active in economic espionage.[39] Companies are still fearful of the IP loss risks incurred by partnering with Chinese firms. The 2016 China Business Climate Survey Report shows that over 50% of the companies believe that the risks of IP theft and data security are greater in China than any other market in which the company operates.[40] This survey also shows that unclear laws and inconsistent regulatory interpretation are the top challenges and business concerns.[41] It should come as a no surprise then that 60% of the companies surveyed found China's enforcement of trade secrets as ineffective or very ineffective even though nearly half were satisfied with the IPR laws and regulations themselves.[42]

Companies, by themselves, are at a distinct disadvantage in their ability to protect their virtual IP especially against state-run intelligence resources. In order to offset some of this disadvantage, E.O. 13691 - Promoting Private Sector Cybersecurity Information Sharing was enacted in 2015. Executive orders are directives issued by the President, generally to govern actions of Federal Agencies and "may have the force and effect of law."[43] This Executive order permits and encourages the sharing of cyber security information between "private companies, nonprofit organizations, executive departments and agencies, and other entities" in order to respond to risks and threats in near-real time.[44] The order also recognizes that data standards must be developed to effectively share information in real time. The E.O. designated the Secretary of Homeland Security to shepherd the sharing initiatives and chair any standards organizations that may arise.[45] The E.O. also delineates roles and responsibilities for the development of standards. These standards will quickly help protect a larger

number of corporate systems from the theft of virtual IP by simplifying the sharing of threat data.

The network devices that help defend virtual IP, such as firewalls and intrusion protection systems, operate based on syntactically specific rules. These rules manage the flow of data, such as blocking access to gambling websites or preventing malicious actors from accessing a company's network. For example, a network administrator that discovers malware that is exfiltrating virtual IP can develop a specific rule to block the malware from stealing the data. If that rule, however, conforms to a DHS standardized format, the administrator, then, could send the rule around the world whereby the rule could be utilized by other network protection devices. This would result in near-real time protection of other networks. This process would dramatically increase the speed and efficiency of network protection and leverage the collective efforts for the benefit of everyone. This rule sharing is somewhat analogous to the AMBER alert system, where in a matter of minutes anyone driving down a major highway is informed about an abducted child and alerted to the specific details, such as vehicle make, model and license plate number. The data used by the Amber alert system are standardized and formatted in such a way that every system that displays the alert (road signs, smartphones, and television broadcasts) can process the data. This increases the number of people to watch for the vehicle, and contact authorities if detected. However, with respect to E.O. 13691, the government does not mandate nor advocate for a particular model or standard for information sharing.

Since there is no nationwide standard, there are at least nine industry, academia, and government "standards" for enabling cyber threat information sharing.[46] Each

standard has merits and arose to meet specific needs. Yet, cyber threats morph rapidly and to counter these threats, companies must rapidly share data. Imagine the confusion if the AMBER alert system used multiple standards for displaying abduction data. For instance, on one highway, the vehicles identification number (VIN) is displayed instead of the license plate, or perhaps the data is displayed in a language other than English. Not having a standard or having multiple standards reduces the effectiveness and limits the ability to share threat data in a meaningful way.

Given that the current state of virtual IP protection is still inadequate, the remainder of this paper will focus on the following two recommendations to improve virtual IP protection; increase federal resources to investigate and prosecute virtual IP theft, and mandate federal standards for government agencies and that produce cyber threat information.

The first recommendation endorses and expands the IP Commission Report suggestion to increase FBI and DOJ resources to investigate and prosecute virtual IP theft.[47] The FBI is the primary law enforcement agency for matters of serious cybercrimes and national security with respect to cyber espionage. However, as the IP Commission Report notes, there has been a dramatic increase in cyber-enabled trade secret theft.[48] This increase in virtual IP theft outpaces the FBI's capacity to investigate and DOJ's ability to prosecute crimes. As a result, the FBI and DOJ require additional resources to meet the investigative and prosecutorial demands. However, the recommendation does not include increasing resources for state and local law enforcement because of legal, jurisdiction and attribution issues. As the fields of cyber

forensics, cyber investigations and cyber law mature, it may warrant revisiting state and local law enforcement roles.

The increase in FBI resources will enable the FBI to investigate virtual IP theft that occurs at smaller businesses and start-ups. As noted by Blair and Huntsman, these small businesses and start-ups are "an indispensable part of the United States' culture of innovation, are being increasingly targeted by IP thieves, and have fewer resources to defend themselves."[49] Not only do they have fewer defensive resources, generally, they are least able to absorb financial losses as a result of stolen IP.

To expand on the IP Commission's suggestion, we recommend that the FBI and DOJ aggressively publicize prosecutions and convictions of cyber criminals in order to affect this public perception and change cyber behavioral norms. Research has shown that messages showing fines and possible legal prosecution does little to deter illegal cyber activity.[50] However, focusing on arrests and convictions, increases "the perception that there is a high probability of getting caught," and changes the risk calculations.[51]

Complimenting an increase in investigative and prosecutorial resources, the U.S. government must assist the private sector to raise the cyber security defenses of company systems that store virtual IP. E.O. 13691 should be expanded to mandate that federal agencies who produce shareable cyber threat information must provide that information in a standard format and this threat information must be made available to public and private sectors. The DHS Secretary, based on its unique role in securing and protecting government and commercial networks and infrastructure, should select the standard with input from industry and academia. Additionally, DHS will be responsible

for aggregating all the federal agencies' cyber threat data and disseminating the data to anyone that subscribes.

A single published standard will allow for every network security provider to take that information and automatically translate it to a format that their network security device understands, no matter the security device, or proprietary language in which that device communicates. This will enable network security devices to protect networks and virtual IP at near-real time speeds. This model would work much the same way that anti-virus (AV) companies keep their consumer products updated but the focus would be on network protection devices such as firewalls and intrusion prevention devices instead of on individual computers.

Companies that subscribe to DHS' threat information could provide feedback as to the effectiveness of the information, similar to how AV products report metrics such as number and types of malware discovered to the manufacturer. This allows the AV company to understand the scope and magnitude of specific threats. Network devices that use DHS' threat information could also report back to DHS if any of the threat information prevented or halted an intrusion. These metrics would allow DHS to evaluate the effectiveness of the information as well as understand the prevalence of the threat. For instance, assume a specific piece of malware was detected and reported to DHS by twelve separate network devices and these devices belonged to twelve different aerospace companies. This type of information is valuable to understand the threat and to protect specific industries from targeted attacks. And because the data is standardized, this model allows for consumers to contribute observations as well.

Using the previous example, but this time instead of the threat information coming from DHS, it came from one aerospace company that detected a threat while monitoring their network. The company analyzed the threat and formatted an alert into the DHS standard. They provided it to DHS, who, in turn provided it to all of the subscribers and now eleven other companies reported back that they prevented further intrusion attempts. In this example, one company's knowledge helped protect the rest of the community. The power of this model is a direct result of standardized cyber threat data and reinforces the notion that protection of virtual IP and its prevention from theft requires a community and whole-of-government approach.

The scale and magnitude of IP theft threatens the U.S. economy and national security. In order to fully protect all IP, the U.S. must recognize the fundamental differences between physical IP protection and virtual IP protection. Physical IP is protected through multiple rings of defense, well established norms of behavior and a mature legal system to investigate, apprehend and bring to justice those that steal physical IP. Unfortunately, virtual IP does not benefit from these same protections.

The protection of virtual IP suffers from limited rings of defense, immense attribution difficulties and few established cyber norms of behavior. Virtual IP protection is limited to primarily the corporate defenses, such as encryption, firewalls and intrusion detections systems. The difficulties in attribution contribute to a perception that cybercrimes cannot be rigorously enforced, which further undermines behavioral norms. Without the ability to enforce behavioral norms, society cannot deter the theft of virtual IP nor reinforce the emerging international cyber norms of behavior. In recognition of

this issue, the U.S. government developed a comprehensive strategy to protect and secure cyberspace.

The International Strategy for Cyberspace addresses the lack of cyber behavioral norms by establishing U.S. policy and strategy for creating a safe and secure cyber domain, whereby nations and individuals promote cyber norms of behavior and they are held accountable for their actions in cyberspace. To promote international norms, the U.S. recognizes the need for the cooperation of the international community. As a result of this recognition, the U.S. and China agreed that neither country would conduct economic espionage for the benefit of their commercial sectors. The U.S., also demonstrated its resolve to hold malicious actors accountable by indicting five members of the Chinese military for conducting economic espionage.

To continue to reinforce these emerging international cyber norms of behavior the U.S. government should allocate more resources to the FBI and DOJ in order to investigate and prosecute virtual IP theft. Greater capacity to investigate and prosecute virtual IP theft will help protect the more vulnerable smaller and start-up companies. Also, increased public awareness of successful investigations and prosecutions will help deter virtual IP theft and reinforce responsible cyber behavioral norms. However, enforcement is only one aspect, the U.S. government has a responsibility to help companies protect their virtual IP from theft.

A data standard for sharing cyber threat information is required so that companies can protect their virtual IP at near-real time speed. DHS should mandate the standard and provide the mechanism by which the threat information is shared. This

collaboration would increase the network security posture of companies, enable better threat understanding by providing feedback, and leverage community threat analysis.

In conclusion, the theft of IP threatens our economy, national security and ultimately our way of life. The global connectedness has made our virtual IP vulnerable and susceptible to theft. To combat this theft requires innovative, and creative ideas and a concerted effort led by the Federal government.

Endnotes

[1] Josh Rogin, "NSA-Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'," *Foreign Policy: The Cable*, July 9, 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history (accessed November 3, 2016).

[2] Dennis C. Blair and Jon M. Huntsman Jr., *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (Washington, DC: National Bureau of Asian Research, May 2013), 11, http://www.ipcommission.org/report/ip_commission_report_052213.pdf (accessed November 3, 2016).

[3] Ibid., 12.

[4] Ibid., 10.

[5] Peter Andreas, *Smuggler Nation* (New York: Oxford University Press, 2013), 110.

[6] Ibid., 109.

[7] Ibid.

[8] Ibid., 103.

[9] Ibid.

[10] Neal Heath, "Samuel Slater: American Hero or British Traitor?" *BBC News,* September 22, 2011, http://www.bbc.com/news/uk-england-derbyshire-15002318 (accessed January 12, 2017).

[11] Andreas, *Smuggler Nation*, 110.

[12] Ibid., 111.

[13] Ibid.

[14] Ibid.

[15] Ibid., 112.

[16] Blair and Huntsman, *The IP Commission Report*, 1.

[17] Kirk R. Williams and Richard Hawkins, “Perceptual Research on General Deterrence: A Critical Review,” *Law & Society Review* 20, no. 4 (1986): 545.

[18] Kirsten Robertson et al., "Illegal Downloading, Ethical Concern, and Illegal Behavior," *Journal of Business Ethics* 108, no. 2 (June 2012): 221.

[19] Ibid.

[20] Ibid., 222.

[21] Ibid., 221.

[22] “[T]he authors developed a consumer ethics scale that examined consumer ethical beliefs regarding various questionable behaviors. They further linked these consumer beliefs to demographic and attitudinal information. Their research resulted in a four dimensional solution for consumer ethical beliefs: (1) actively benefiting from illegal activities, (2) passively benefiting, (3) actively benefiting from deceptive (or questionable, but legal) practices, and (4) no harm/no foul activities.” Scott J. Vitell, and James Muncy, "The Muncy-Vitell Consumer Ethics Scale: A Modification and Application," *Journal of Business Ethics* 62, no. 3 (2005): 267.

[23] Ibid., 222.

[24] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units,” February 19, 2013, 3, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (accessed March 5, 2017).

[25] Ibid., 4.

[26] Ibid., 3.

[27] Barack H. Obama, *International Strategy for Cyberspace*: *Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011).

[28] Ibid., 17

[29] Ibid., 25.

[30] Ibid., 18.

[31] U.S. Department of Justice, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage,” May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (accessed January 20, 2017).

[32] Ibid.

[33] Ibid.

[34] The White House Office of the Press Secretary, “FACT SHEET: President Xi Jinping’s State Visit to the United States,” September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (accessed January 20, 2017).

[35] Blair and Huntsman, *IP Commission Report*, 15.

[36] Amy Chang, "Warring States: China's Cybersecurity Strategy," December 3, 2014, 7, https://www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy (accessed March 5, 2017).

[37] John Hayword, "Chinese Military Hackers Intimidated by DOJ Indictments, U.S. Officials Say," December 2, 2015, http://www.breitbart.com/national-security/2015/12/02/chinese-military-hackers-intimidated-doj-indictments-u-s-officials-say/ (accessed March 5, 2017).

[38] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 3.

[39] U.S. Trade Representative, *Special 301 Report* (Washington, DC: U.S. Trade Representative, April 2016), 20.

[40] American Chamber of Commerce in the People’s Republic of China, *2016 China Business Climate Survey Report 2016* (Beijing: American Chamber of Commerce in People’s Republic of China, 2016), 42, http://www.bain.com/Images/2016_China_Business_Climate_Survey_Report.pdf (accessed January 12, 2017).

[41] Ibid., 18.

[42] Ibid., 41.

[43] John Contrubis, *Executive Orders and Proclamations* (Washington, DC: U.S. Library of Congress, Congressional Research Service, March 9, 1999), 1.

[44] Barack H. Obama, *Promoting Private Sector Cybersecurity Information Sharing*, Executive Order 13691 (Washington, DC: The White House, February 20, 2015), 9349.

[45] Ibid.

[46] The most commonly used cyber threat information standards are, Open Threat Exchange (OTX), Structured Threat Information Expression (STIX), Collective Intelligence Framework (CIF), Open Indicators of Compromise (OpenIOC) framework, Trusted Automated eXchange of Indicator Information (TAXII), Traffic Light Protocol (TLP), Cyber Observable eXpression (CybOX), Incident Object Description and Exchange Format (IODEF), Vocabulary for Event Recording and Incident Sharing (VERIS). Dave Shackleford, *Who's Using Cyberthreat Intelligence and How?* (Bethesda, MD: Sans Institute, February 2015), 19, https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767 (accessed February 20, 2016).

[47] Blair and Huntsman, *IP Commission Report*, 5.

[48] Ibid., 67.

[49] Ibid.

[50] Robertson et al., "Illegal Downloading, Ethical Concern, and Illegal Behavior," 223.

[51] Ibid.