Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad

National Intellectual Property Rights Coordination Center

November 2011

EXECUTIVE SUMMARY

Introduction

The continuing development and protection of intellectual property (IP) is of critical importance to the United States. As President Barack Obama has noted, "Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century." Although there is no consensus regarding the current value of United States rights holders' IP (United States or American IP), the value is estimated to be in the hundreds of billions to trillions of dollars. Protecting this valuable resource against theft is important not only because of its significant economic value, but because of the threat intellectual property rights (IPR) violations pose to the health and safety of the American public, the integrity of American critical infrastructure, and American national security.

To effectively protect American IP, the United States government must understand the myriad threats posed by IP theft. To further this understanding, the National Intellectual Property Rights Coordination Center (IPR Center) analyzed the global threat to United States interests from criminal IPR violations. This analysis examines the nature of the threat, its magnitude, the types of offenders committing these offenses, and its source. It analyzes the many detrimental effects of IP theft, including the danger to the public's health and safety, economic losses to rights holders and the government, the undermining of America's national security, and the potential funding of organized crime and terrorist organizations. It also focuses on selected industries because of their significance related to these interests, including aircraft parts, content piracy, electronics, luxury goods, and pharmaceuticals. Finally, because of their overall significance in the threat picture, it focuses on the threat from offenders in China, India, Russia, the tri-border area of South America (TBA),[*] and the United States. This analysis is not intended to be exhaustive but rather characterize the threat with sufficient specificity to guide the law enforcement response.

To prepare this analysis, the IPR Center established domestic and international teams to conduct research and interview IPR experts in the United States, China, and India. In total the domestic and international teams interviewed 126 IPR experts in government, industry, and academia. The domestic team analyzed relevant United States Intelligence Community (USIC) reporting, information from federal law enforcement investigations, industry generated reports, and other open source research.[**]

[*] The TBA is the intersection of Argentina, Brazil, and Paraguay.
[**] The information cut-off date for this report was May 13, 2011.

Key Findings

- The threats to United States IP interests are immense and growing both in size and scope.
- IP theft negatively affects the economic well-being of United States rights holders through lost profits, brand dilution, and enforcement costs, and the United States' economic well-being through job and tax revenue losses.
- Some counterfeits, such as pharmaceuticals and aircraft and automotive parts, pose threats to the public's health and safety.
- Certain IPR violations, including computer network exploitations from pirated software, counterfeit parts on military equipment, and theft of sensitive United States trade secrets, pose threats to the United States' national security, including its war fighters.
- The types of products being counterfeited and the techniques used to counterfeit them are becoming more sophisticated.
- The threat is shifting from the secondary market, where consumers know they are purchasing infringing goods, to the primary market where retailers deceive them into believing they are buying genuine goods.
- Counterfeiters increasingly are finding ways to exploit supply chain vulnerabilities or develop alternative supply chains to evade the standards that ensure supply chain integrity.
- The substantial increase in worldwide use of the Internet has fueled the threat, giving counterfeiters increased access to customers, facilitating deception regarding the nature of the goods offered, and altering the ways in which infringing goods move from their source to the consumer. In particular, use of the Internet has increased the availability of counterfeit pharmaceuticals and digital piracy of music, movies, and software in the United States and elsewhere.
- Although there are multiple reasons why actors commit IPR violations, earning a profit remains the principal motivator across the various types of actors involved. Offenders also perceive IP theft to be a low risk crime because they believe both the likelihood of apprehension and possible penalties if prosecuted are relatively low compared to other "more serious" offenses, such as violent crimes and drug trafficking.
- A variety of types of offenders participate in IPR violations including: individuals and small groups; members of general criminal enterprises, as well as their subset organized crime groups; supporters of terrorist organizations; members of gangs; foreign government actors; and members of warez groups. These offenders are involved in various phases of the manufacturing, distribution, and sales of infringing goods.
- The role of criminal organizations, including organized crime and gangs, in IP theft has expanded along with the increasing sophistication of the counterfeiting business and easy access to profits.
- Most physical infringing goods are produced overseas and cross United States borders to reach consumers in the United States.
- Offenders in many countries pose a threat, but China-based offenders are the dominant threat and dwarf all other international threats.
- Although the majority of infringing physical goods consumed in the United States are manufactured overseas, extensive piracy of copyrighted music, movies, and software and distribution and sales of imported infringing goods occurs in the United States.

- Theft of trade secrets from United States companies is most often committed within the United States by United States actors. China-related offenders are the most common international threat to United States trade secrets.

The Nature of the Threat

The threat to United States IP is multifaceted and growing. Infringing goods traditionally were limited to luxury goods, such as counterfeit handbags and watches. With the advent of new technologies, combined with the high profits and perceived low risk from selling infringing goods, counterfeits have become increasingly more sophisticated and prevalent. Products in every industry – from food to health care products to electronics – now are being counterfeited. Law enforcement officials have to date seized over 600 different categories of infringing goods in the United States.

In recent years the supply for infringing goods has shifted from the lower profit secondary market – where consumers know they are purchasing counterfeit goods and so demand a significantly lower price – to the primary market – where consumers will pay higher prices because counterfeiters deceived them into believing they are purchasing genuine goods. Offenders are able to deceive consumers because of improvements in the appearance of infringing goods. Some infringing goods so closely resemble the genuine products that the two are indistinguishable to the naked eye.

Counterfeiters may produce infringing goods – meaning those that either infringe on trademarks or pirate copyrighted materials – using a variety of methods. They may create infringing goods in facilities ranging from "mom and pop" home-based factories to sophisticated clones of legitimate factories producing genuine goods. They may arrive in the United States domestic market by a variety of means, ranging from containers shipped by sea to mail packages shipped by air to goods smuggled across the border. In an attempt to avoid detection by customs officials, offenders are shifting from shipping infringing goods in large containers to using smaller, discrete packages to import their infringing goods into the United States. This change is particularly noticeable with counterfeit pharmaceuticals.

The widespread availability of the Internet has contributed to the increasing threat. The Internet enables manufacturers to sell infringing products to customers around the world. The Internet facilitates counterfeiters who wish to breach or avoid legitimate supply chains for products. The impact of the Internet is particularly noticeable in the pharmaceutical, automotive parts, and electronics industries. Offenders are creating websites that appear legitimate, deceiving consumers into purchasing infringing goods. Because of the anonymity of the Internet and the ability of counterfeiters to disguise the true nature of the goods they offer online, consumers are hampered in their ability to make rational choices. The Internet also has made pirated content, specifically music, movies, and software, widely and easily available.

The Magnitude of the Threat

There have been several attempts to quantify the magnitude of the threat, but due to its multi-dimensional nature this task is impossible to do with any precision. Measures of the threat must

account for the varying types of infringing goods being sold, the rate at which consumers substitute purchases of infringing goods for genuine goods, and the differing types of economic harm. There are also health and safety costs as well as national security concerns. Although impossible to measure precisely each of these components, the available evidence suggests the negative economic impact of IPR violations worldwide are in the hundreds of billions of dollars and trending upward.

The economic damage caused by IP theft varies by industry but for some they are extensive. For example, the recording industry estimates 63 percent of the music obtained by end users in the United States is pirated. Industry estimates that music and movie piracy rates in China are around 90 percent. Economic losses from business software piracy are in the billions of dollars. It is estimated that approximately 50 percent of the pharmaceuticals on worldwide illegal websites are counterfeit. In addition to lost sales, rights holders risk loss of brand value and incur heavy costs to protect their IP. The United States loses tax revenue, customs duties, and jobs when consumers purchase infringing goods.

In addition to economic losses to industry and the government, consumers face serious health and safety risks from infringing goods. Counterfeit pharmaceuticals may contain a dangerous incorrect dosage of medication or harmful contaminants. Although Pfizer's Viagra is reported to be the most counterfeited pill in the world, counterfeiters have expanded operations to include cholesterol drugs, cancer drugs, AIDs drugs, and anti-malarial medicines. Automobile parts may make vehicles unsafe, aircraft parts may fail in flight, or electrical components may catch fire. Because these products are often technical in nature, average consumers are incapable of determining whether the goods they purchase pose a risk or the nature of the risk. There is also a threat to national security from system failures or breaches of sensitive systems through back doors opened by pirated software or counterfeit components. Currently there are no verifiable measurements of the actual impact these additional dimensions of the threat cause, but there is no question these threats exist and could have potentially catastrophic impacts.

Offenders

The primary motivation for committing IPR violations is profit. Counterfeiting is a highly profitable crime and it is likely to become even more lucrative with the shift to the higher priced primary market. Offenders also perceive these crimes to be low risk as they believe both the likelihood of apprehension and possible penalties if prosecuted are relatively low for these crimes compared to other "more serious" offenses, such as violent crimes and drug trafficking.[*] Other motivations include a desire to steal sensitive United States information, vengeance, and fame.

Several types of offenders participate in IPR violations: small independent operators, members of general criminal enterprises, members of organized crime groups, supporters of terrorist organizations, members of gangs, foreign government actors, and members of warez groups.[**]

[*] The Administration recently proposed increasing sentences for IP theft crimes to alter the risk/reward calculations of potential offenders.

[**] Warez groups specialize in the illegal online distribution of copyrighted content (e.g. business and entertainment software, movies, and music).

These offenders may be members of a criminal organization or, in the case of terrorist organizations, supporters who provide funds to further the organization's cause. These offenders are involved in various phases of the manufacturing, distribution, and sales of infringing goods. Although it is likely some offenders use profits from IP theft to fund other criminal activity, a lack of visibility into their finances prevents a direct linkage between them.

The Source of the Threat

Offenders in foreign countries are the principal source of the threat to United States IP. Production of infringing goods is conducted primarily outside the United States and these items may cross numerous borders prior to delivery to consumers in the United States. The one notable exception is the production of pirated works in the United States for domestic production.

The magnitude and type of threat to United States interests varies from country to country. Offenders in China pose the greatest threat to United States interests in terms of the variety of products infringed, the types of threats posed (economic, health and safety, and national security), and the volume of infringing goods produced there. The majority of infringing goods seized by CBP and ICE originated in China. Offenders in China are also the primary foreign threat for theft of trade secrets from United States rights holders.

China's push for domestic innovation in science and technology appears to be fueling greater appropriation of other country's IP. The U.S.-China Economic and Security Review Commission (China Commission) has cautioned that China's approach to faster development of sophisticated technology has included the "aggressive use of industrial espionage." As the globalization and growth of multinational corporations and organizations blurs the distinction between government and commerce, it is difficult to distinguish between foreign-based corporate spying and state-sponsored espionage. Although most observers consider China's laws generally adequate for protection of IPR, they believe China's enforcement efforts are inadequate. Despite some evidence of improvement in this regard, the threat continues unabated.

Offenders in India are notable primarily because of their increasing role in producing counterfeit pharmaceuticals sent to consumers in the United States. Offenders in the tri-border area of South America are a noteworthy threat because of the possible use of content piracy profits to fund terrorist groups, notably Hizballah. The most significant threat to United States interests from offenders in Russia is extensive content piracy, but this is principally an economic threat as the pirated content is consumed domestically in Russia.

Distribution and sales of infringing goods are the principal IPR violations in the United States. Except for pirated content, there is limited domestic production of infringing goods. Physical pirated content is commonly produced in the United States because it is more cost effective to create this content domestically than import it from overseas. Printing of sports apparel and paraphernalia for last minute sports events, such as the World Series or Super Bowl, also is common in the United States because there is not enough time to import these goods from other countries. Offenders in the United States are also the primary source of trade secret theft from United States rights holders.

Conclusion

The threat to United States interests from IP theft has evolved. No longer confined to cheap knockoffs of luxury goods, IP theft is putting American industry and the public at risk of significant economic and/or safety and health consequences. These violations also place United States national security, including United States war fighters, at risk.

This multi-dimensional threat is not confined to particular industries or countries and will increase for the foreseeable future. Production and distribution of infringing goods are a steady and significant revenue source for a broad array of offenders. The lower risk and higher profits from IPR offenses compared to other offenses will continue to draw individuals to commit IPR crimes. The trend toward producing goods for the more profitable primary market serves only to make IP theft more lucrative.

This movement to the primary market will also exacerbate the potential health and safety consequences from counterfeit goods as unwitting purchasers underestimate the risks associated with these goods. The increasing significance of Internet transactions enhances the ability of criminals to penetrate the primary market. In addition, the Internet facilitates circumvention or infiltration of legitimate supply chains in ways that can confuse or deceive consumers. Supply chain risks are evident across a broad array of industries and customers.

This multi-dimensional threat requires a multi-dimensional response. No industry or country is immune from the threat, nor can they address the threat alone. It calls for increased cooperation among those it affects, as well as increased resources and improved tools to tackle the growing and evolving nature of the threat. The threat also calls for better education regarding the risks it poses and how to defend against it. The following analysis will provide a detailed basis for developing more strategic and effective responses to the burgeoning threat.

I. INTRODUCTION

The Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act) directed that an analysis of the threat posed by intellectual property rights (IPR) violations – including the costs to the United States economy and threats to health and safety – be prepared.[1] In accordance with this directive, the National Intellectual Property Rights Coordination Center (IPR Center) prepared this global analysis of the threat from intellectual property theft to the United States. The IPR Center is an interagency task force established and led by the Department of Homeland Security (DHS) Immigration and Customs Enforcement – Homeland Security Investigations (ICE-HSI) to provide a unified response by United States law enforcement to the growing threat of global counterfeiting.[*2]

A. Scope

This analysis examines the threat from criminal IPR violations – copyright, trademark, and theft of trade secrets offenses – that pose a danger to United States interests with a particular emphasis on the economic interests of United States rights holders, the United States economy at large, the public's health and safety, and threats to national security. It also examines the national security implications of organized crime and terrorist supporters' involvement in IP theft. In addition to the threat within the United States, this global analysis focuses on the threat posed by offenders in China, India, Russia, the Tri-Border Area (TBA) of South America,[**] and the United States because of their relative importance in the overall threat picture. This analysis also focuses on selected industries based on the relative extent of violations occurring in that industry and/or their significance related to the key interests identified earlier. The industries are aviation, computer software, electrical components, luxury goods, music and video content, and pharmaceuticals. This analysis is not intended to be exhaustive, but rather to characterize the threat with sufficient specificity to permit national law enforcement to effectively address the threat and identify critical intelligence gaps for further collection and analysis.

[*] In addition to ICE-HSI, the IPR Center has representation from the following domestic agencies: United States Customs and Border Protection (CBP); the Federal Bureau of Investigation (FBI); the United States Food and Drug Administration Office of Criminal Investigation (FDA-OCI); the United States Postal Inspection Service (USPIS); the Department of Commerce (DOC) – International Trade Administration; the United States Patent and Trademark Office (USPTO); the United States Naval Criminal Investigative Service (NCIS); the Defense Criminal Investigative Service (DCIS); the Consumer Product Safety Commission (CPSC); the United States Army Criminal Investigative Command (CID) – Major Procurement Fraud Unit; Defense Logistics Agency (DLA) – Office of Inspector General; the United States Department of State – Office of International Intellectual Property Enforcement; the United States General Services Administration (GSA) – Office of Inspector General; United States Air Force Office of Special Investigations; National Aeronautics and Space Administration (NASA) – Office of Inspector General; and INTERPOL's United States National Central Bureau. In addition, the IPR Center has international partners, including representatives from the Government of Mexico –Tax Administration Service (Mexican Revenue Service) and the Royal Canadian Mounted Police. The IPR Center also works closely with the United States Department of Justice (DOJ) Computer Crime and Intellectual Property Section (CCIPS).

[**] The TBA is the intersection of the Argentina, Brazil, and Paraguay borders.

B. Definitions

The scope of this analysis is limited to criminal violations of IPR. IPR may be in the form of patents, trademarks, copyrights, and/or trade secrets (see box). Although the definitions of these rights are fairly straightforward, what constitutes a violation of these rights is less so. Both the literature the analytic team reviewed and the IPR experts the team interviewed interchangeably used terms such as "counterfeit," "pirated," "substandard," "nonconforming," "generic," "unapproved," "fraudulent," "spurious," "suspect," "improperly modified," or "diverted" when discussing the threat.

Intellectual Property Rights Definitions

Trademark*: Distinctive word, name, symbol, device, or combination thereof used by a brand owner to uniquely identify and distinguish his or her goods from those manufactured or sold by others and to indicate the source of the goods. Criminal law governs the trafficking in goods bearing a counterfeit mark.*

Copyright*: A set of exclusive rights given for a limited time to the creator of an original work of authorship in any tangible medium of expression. These include the right to reproduce, distribute, publicly perform, publicly display, make derivative work, and make digital audio transmissions of sound recordings Criminal law governs the unauthorized reproduction and distribution of copyrighted works.*

Trade Secret*: Information, such as a formula, pattern, device, or compilation of information used in a business that the owner has taken reasonable steps to keep secret and it has independent economic value because it is secret. Criminal law governs the misappropriation of a trade secret to benefit someone other than the owner, or in the case of economic espionage, the misappropriation of a trade secret to benefit a foreign instrumentality or government.*

Patents*: Right granted by the government to the inventor for an invention to exclude others from making, using, and selling devices that embody the invention. Patents may only be enforced by the rights holder through civil processes.*

Counterfeit Goods*: Any goods, packaging, or labels that bear a mark that is identical to or is substantially indistinguishable from a trademark validly registered for those goods and that has been applied to such goods, packaging, or labels without the trademark holder's authorization.*

Pirated Works*: Copies of copyrighted works that are made without the copyright holder's authorization.*

Infringing Goods*: Term used within this report to refer jointly to counterfeit goods and pirated works.*

Sources: U.S. Department of Justice, Computer Crime and Intellectual Property Section, *Prosecuting Intellectual Property Crimes, Third Edition*, Sept. 2006, 3-5; Government Accountability Office, "Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods," Apr. 2010, 6.

This analysis, however, focuses on criminal IPR violations as opposed to general contractual rights or other frauds. Thus, this analysis is not concerned with conduct associated with gray market, diverted goods, generics, or factory overruns. These activities may involve breaches of contractual relationships between the rights holders and their manufacturers, distributors, or sellers but they do not generally violate criminal IPR laws.[3] In addition, because the threat is being viewed through a law enforcement lens, this analysis only tangentially discusses patent issues, which are enforced primarily by rights holders using civil processes. This analysis, therefore, focuses principally on counterfeit goods, pirated copyrighted works, and theft of trade secrets.

One definitional distinction important for understanding the nature of the threat is the difference between the primary and secondary markets for infringing goods. The primary market involves infringing goods that are intended to deceive the consumer into believing they are receiving the genuine product. The secondary market involves infringing goods where the consumer knows or should know he or she is purchasing a counterfeit or pirated good. This distinction will be a significant factor in assessing several dimensions of the threat.

C. Methodology

This analysis is based on the judgment of teams working for the United States government. Research, evaluations, interviews, and other activities in support of this analysis were conducted in the United States, China, and India. A domestic team based at the IPR Center interviewed 71 relevant government officials, rights holder representatives, and academic experts. These individuals were selected for interviews based on their roles in particular government organizations, selected industries, or academic areas of interest and expertise. The team researched existing government materials, including United States Intelligence Community (USIC) reporting, information from federal law enforcement investigations, other controlled government reporting, and open source research.[*] In addition, the FBI's IPR Unit temporarily detailed (TDY) two teams, each consisting of an FBI Special Agent and an Intelligence Analyst, to Beijing, China (TDY China Team) and New Delhi, India (TDY India Team) to gather relevant information by interviewing United States government officials, industry representatives, and, where possible, foreign government officials. These teams conducted 55 interviews. The domestic team also received assistance from a team of open source researchers.

IPR Experts Interviewed

Total: 126

International TDY Teams: 55
Domestic IPR Analysis Team: 71
Government: 65
Industry: 59
Academia: 2

Source: IPR Threat Report Team

II. KEY QUESTIONS

- What methods are being used to violate United States IPR?
- What are the leading drivers of the demand for infringing goods?
- Are there notable trends in the methodologies used to commit IPR violations?
- What is the magnitude of the threat posed by violations of United States IPR?
- What economic interests are threatened by violations of United States IPR?
- What are the health and safety consequences caused by violations of United States IPR?
- What are the national security implications from violations of United States IPR?
- Who are the principal offenders behind the threat to United States IPR?
- What are the motivations for violating United States IPR?
- Is there a nexus between organized crime or criminal enterprises and IPR violations?
- Are profits from IPR violations used to fund terrorist organizations?
- Where is the threat originating?

[*] All information cited and presented in this report is unclassified. Classified information may alter or improve upon the conclusions made in this report. The information cut-off date for this report was May 13, 2011.

III. KEY FINDINGS

- The threats to United States IP interests are immense and growing both in size and scope.
- IP theft negatively affects the economic well-being of United States rights holders through lost profits, brand dilution, and enforcement costs, and the United States' economic well-being through job and tax revenue losses.
- Some counterfeits, such as pharmaceuticals and aircraft and automotive parts, pose threats to the public's health and safety.
- Certain IPR violations, including computer network exploitations from pirated software, counterfeit parts on military equipment, and theft of sensitive United States trade secrets, pose threats to the United States' national security, including war fighters.
- The types of products being counterfeited and the techniques used to counterfeit them are becoming more sophisticated.
- The threat is shifting from the secondary market, where consumers know they are purchasing infringing goods, to the primary market where retailers deceive them into believing they are buying genuine goods.
- Counterfeiters increasingly are finding ways to exploit supply chain vulnerabilities or develop alternative supply chains to evade the standards that ensure supply chain integrity.
- The substantial increase in worldwide use of the Internet has fueled the threat, giving counterfeiters increased access to customers, facilitating deception regarding the nature of the goods offered, and altering the ways in which infringing goods move from their source to the consumer. In particular, use of the Internet has increased the availability of counterfeit pharmaceuticals and digital piracy of music, movies, and software in the United States and elsewhere.
- Although there are multiple reasons why actors commit IPR violations, earning a profit remains the principal motivator across the various types of actors involved. Offenders also perceive IP theft to be a low risk crime because they believe both the likelihood of apprehension and possible penalties if prosecuted are relatively low compared to other "more serious" offenses, such as violent crimes and drug trafficking.
- A variety of types of offenders participate in IPR violations including: individuals and small groups; members of general criminal enterprises, as well as their subset organized crime groups; supporters of terrorist organizations; members of gangs; foreign government actors; and members of warez groups. These offenders are involved in various phases of the manufacturing, distribution, and sales of infringing goods.
- The role of criminal organizations, including organized crime and gangs, in IP theft has expanded along with the increasing sophistication of the counterfeiting business and easy access to profits.
- Most physical infringing goods are produced overseas and cross United States borders to reach consumers in the United States.
- Offenders in many countries pose a threat, but China-based offenders are the dominant threat and dwarf all other international threats.

- Although the majority of infringing physical goods consumed in the United States are manufactured overseas, extensive piracy of copyrighted music, movies, and software and distribution and sales of imported infringing goods occurs in the United States.
- Theft of trade secrets from United States companies is most often committed within the United States by United States actors. China-related offenders are the most common international threat to United States trade secrets.

IV. THE NATURE OF THE THREAT

A. The Threat Landscape

President Barack Obama summed up the significance of IP to the United States when he said, "In America, innovation doesn't just change our lives. It is how we make a living."[4] Indeed, the United States has long recognized the inherent value of IP, encouraging innovation in Article 1, Section 8 of the Constitution. However, as Intellectual Property Enforcement Coordinator Victoria Espinel, testified, "It takes effective intellectual property enforcement to ensure that a revolutionary idea can blossom into economic opportunity and to allow the American innovative spirit to create the good, high-paying jobs that will drive our prosperity in the 21st Century."[5] Effective enforcement in turn requires understanding the nature of the threat.

Although there is no consensus regarding the current value of United States IP, estimates vary from the hundreds of billions to trillions of dollars.[*] As of 2008, over 18 million Americans were employed in "IP-intensive" industries.[6] These statistics demonstrate at a basic level the sheer magnitude of the value of IP to the United States, and the enormity of the potential economic losses from IPR violations. In addition to economic losses to industry, significant other consequences from IP theft affect the United States. United States consumers, industries, government, and economy all suffer negative effects from IP theft. An analysis of the magnitude of the threat to United States IP is in Section V of this report.

Infringing goods traditionally have been limited principally to counterfeit luxury goods, such as handbags and watches. However, with the advent of new technologies, combined with the high profits and perceived low risk from selling infringing goods, counterfeits have become increasingly more sophisticated and prevalent. Any brand in any industry is now at risk of being counterfeited. Over 600 different categories of infringing goods have been seized in the United States and the number of categories is expected to continue to expand.[7]

Improvements in the overall technology for manufacturing infringing goods have made IPR violators capable of producing counterfeit goods that resemble genuine products so closely that

[*] For example, one report contended American IP is worth over $5 trillion — "more than the nominal GDP of any other country in the world." See Global Intellectual Property Center, "Learn About IP," 2010, http://www.theglobalipcenter.com/pages/why-are-intellectual-property-rights-important. One study estimated the gross domestic product (GDP) in the core copyright industries (namely, motion picture, business and entertainment software, and publishing industries) in 2005 was $819.06 billion, which equals 6.56 percent of the 2005 United States economy. See Stephen E. Siwek, "Copyright Industries in the U.S. Economy," 2006, 2, http://www.iipa.com/pdf/2006_siwek_full.pdf.

they are, to the naked eye, indistinguishable from the genuine products.[8] One source noted that even holograms, which are intended to be a significant security device, "are being perfectly imitated, which increases the complexity of identifying the counterfeited items."[9] Only after expert review, such as X-raying the goods, can the inaccuracies in the designs be discovered and the products determined to be counterfeit.[10] The high caliber of counterfeiting technology also has contributed to an increase in the variety of products being counterfeited. Products from technical industries, including electronics, automotive, and aircraft parts, are now being counterfeited with such resemblance to legitimate goods that the infringing goods are able to successfully infiltrate legitimate supply chains to be sold to unsuspecting consumers.[11] Other infringing goods, such as luxury goods, pharmaceuticals, and multimedia content, are rarely sold in the legitimate supply chain, but can be purchased easily in the secondary market.

B. The Infringement Process

1. Production and acquisition of infringing material

As described in the Landscape section above, IPR violators are using increasingly sophisticated methods to produce and distribute their infringing goods. There is no standard method for producing infringing goods, regardless of the country the goods are produced in or the types of goods being produced. This section will provide an overview of some of the most common methods used to produce infringing goods or acquire infringing material, such as trade secrets.

Small factories

Counterfeit clothing and luxury goods traditionally are manufactured overseas in unsophisticated factories. The factories may be as small as a room in someone's house or a small building in a village. The Chinese term for such operations is "shanzhai factory."[12] They often are poorly equipped, family-based operations that produce counterfeit goods. These factories often employ local villagers who make a few dollars a day and most likely have no idea they are engaged in an illegal enterprise. Numerous people may be involved sewing fabric and applying counterfeit labels to clothing or handbags. One industry representative reported counterfeit versions of designer purses may cost these factories less than two dollars each to make.[13] These factories may make counterfeits for local market consumption as well as exportation to other countries, including the United States.

Sophisticated factories

Some IPR violators have such sophisticated counterfeiting methods that they operate factories nearly identical to the legitimate manufacturers. For example, a raid of a factory in China known to be producing counterfeit products uncovered a nearly identical factory to the legitimate one, including floor plans and assembly lines.[14] Another company found counterfeiters who had copied seemingly every aspect of the company, including employees' business cards with the name of the genuine company on them, licensing agreements for factories to make goods with the genuine company name on them, signs at the factory with the genuine company's name, and an entire line of counterfeit products.[15] These factories indicate a high level of technical expertise and investment in the manufacturing process of infringing goods. These factories also indicate potential security breaches and theft of trade secrets from rights holders as these factories could not have been coincidentally constructed so similarly to the legitimate factories.

Domestic product completion

Shipping goods to the United States prior to attaching infringing trademarks is becoming more prevalent. The generic base product is manufactured overseas and sent without any infringing trademarks that would alert inspectors the goods are part of an infringing operation. The labels and other trademark identifiers are shipped separately or produced in the United States and affixed after the goods have cleared customs. This method ensures that the base product is not subject to seizure and only imported infringing labels or marks are at risk.[16] For example, blank shirts may be sent to the United States separately from infringing labels. Labels or other trademarked insignias will be applied to the shirts inside the United States. Similar techniques have been used in the electronics and technology industries.[17]

Relabeling/blacktopping

False labeling, commonly referred to as "blacktopping," is one of the main methods for producing infringing electronics and/or related hardware. Blacktopping involves the remarking of computer chips or circuit boards with new labels to give the impression the parts are new and of a potentially higher quality. These products may be legitimate components, manufactured by a legitimate rights holder, but relabeled is more expensive, higher quality, or newer versions.[18] This allows older used parts to be resold at higher prices. Relabeling is a well-documented technique in China for producing infringing circuit boards and computer chips. It reportedly is used frequently in the Guiyu Electronics Market in southeastern China. Offenders there remove chips from recycled PC circuit boards, clean them in the nearby Lianjiang River, and sell them through businesses in China.[19] There is evidence these "refurbished" items are being sold to consumers in the United States.[20]

Relabeling

Source: "Unauthorized Relabeling," Western Digital Warranty Services.

Relabeling is not always done overseas. Following Hurricane Katrina, many circuit breakers were removed from hospitals and factories due to significant water damage. Unauthorized personnel acquired the faulty items, cleaned and repaired them, applied new labels to the circuit breakers, and then sold them as refurbished or upgraded models.[21]

Reverse engineering

Reverse engineering is the process of taking something apart to determine how it was made or manufactured.[22] Although generally a legal process, it is still illegal to sell the product constructed from reverse engineering under the label of the original manufacturer or if the product is still protected by patent. Reverse engineering may be used on fairly simple products, such as shoes or handbags, or highly technical products, such as cell phones or automotive diagnostic equipment, to make credible counterfeit versions.

Physical multimedia piracy

Piracy is the act of copyright infringement, that is, copying a copyrighted work without the copyright holder's authorization. The two most common types of physical piracy are burned and pressed optical discs (ODs) to create illegal CDs and DVDs. Burned ODs require little financial investment and can be created on almost any modern computer with a CD or DVD burner. Pressed ODs, the method used to produce genuine ODs purchased at legitimate retailers, require expensive manufacturing equipment that can cost between $250,000 and $500,000 per piece.[23] A third type of physical piracy involves the use of external multimedia storage devices, such as hard drives, which allow for the simple transfer of gigabytes (GB)[*] of files containing copies of copyrighted works, including music, movie, or business and entertainment software. An offender may preload an external multimedia storage device with pirated content and sell the device with the infringing content, or may upload pirated content onto a customer's personal device. Physical piracy can be committed in a variety of venues, such as burning discs in a small apartment, uploading pirated content onto external multimedia devices in a basement, or actual factories with several disc presses. These goods are sold primarily in street markets, flea markets, or small storefront shops.

Online piracy

Online piracy of multimedia content involves the illegal reproduction and distribution of copyrighted works over the Internet. Online piracy generally occurs through peer-to-peer (P2P) networks, cyberlockers, streaming websites, and/or mobile piracy.[**] Pirated movies uploaded to the Internet for distribution, particularly pre- or newly released movies, are obtained principally

[*] An 80 GB hard drive can store up to 20,000 digital songs in MP3 file format.

[**] Peer-to-peer networks allow users connected to the Internet to link their computers with other computers around the world. These networks are established for the purpose of sharing files. Cyberlockers are Internet hosting services for large static content files. Streaming websites allow users to listen to or view content on demand without downloading files to their computer. Mobile piracy is the streaming and downloading of pirated content to an individual's laptop or mobile phone.

by illegal camcording.[*24] Illegal copies of songs are typically downloaded from legitimate CDs – a process known as "ripping" – and uploaded to the Internet without the consent of copyright holder. Illegal copies of business or entertainment software also may be uploaded onto cyberlockers or P2P networks to allow for mass consumption. Although a less common method of acquiring the original multimedia content, individuals may hack into computers or physically steal media content and subsequently upload this content to the Internet.[25]

Theft of trade secrets

One of the most common methods for stealing trade secrets from United States rights holders is a current or former employee of a United States company transferring files containing the company's trade secrets or other proprietary information onto a portable storage device, such as a USB drive or CD. A study by Symantec and the Ponemon Institute surveyed employees who lost or left a job in 2008. Fifty-three percent of individuals who took company information downloaded it onto a CD or DVD, 42 percent onto a USB drive, and 38 percent sent attachments to a personal email account.[26] For example, one individual copied over 4,000 sensitive Ford documents onto an external hard drive the day before he left the company.[27] In other cases, employees remotely accessed sensitive trade secret files and downloaded them onto a personal laptop or intentionally emailed sensitive trade secrets to unauthorized personnel. For example, an employee was charged with stealing over $1 billion worth of Intel trade secrets by remotely accessing Intel's network, downloading trade secret files, and decrypting them on his personal computer.[28] In rare instances, individuals may physically remove hard copies of trade secret documents.[29]

Trade secrets also may be stolen through computer intrusions. These intrusions may be conducted from computers anywhere in the world and need not be linked to an individual with insider access. Regardless of whether the trade secrets are obtained by an insider or by an outsider using electronic means, if a government entity either directs or benefits from the theft, the case becomes a matter of economic espionage.

2. Moving infringing goods to the United States market

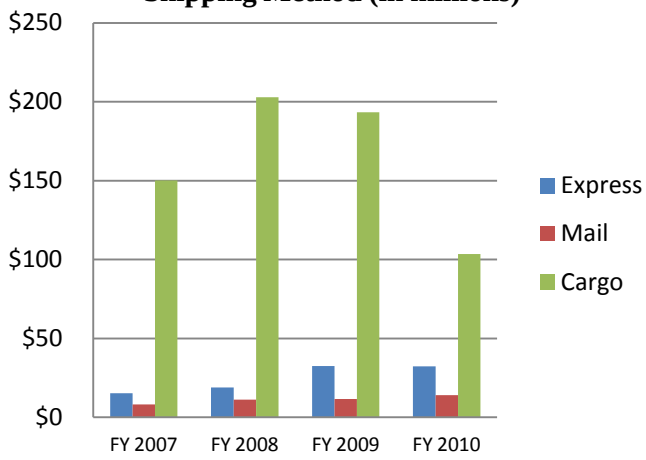
After products have been manufactured they are distributed to the end consumer. As this report is focused on threats to the United States, this analysis focuses on methods of distribution to import infringing goods into the United States. The four main methods used to import goods to the United States are cargo containers shipped by air and sea, individual packages sent through mail centers, packages shipped using express consignment, and digital distribution of pirated content via the Internet.

As shown in Figure 1, the largest values of infringing goods seized involve goods shipped to the United States in cargo containers via air or sea. These containers enter the United States at various ports, particularly the ports of Los Angeles, Long Beach, and New York/New Jersey.[30] Counterfeiters may use deception to import these containers into the United States. They often

[*] Camcording piracy is the unauthorized recording of a movie using a recording device (e.g. camcorder, picture phone, voice recorder, etc.). Camcording piracy accounts for approximately 90 percent of all piracy of newly released movies.

mislabel shipments and provide false documentation to United States Customs officials. For example, a bulk shipment of counterfeit sneakers may be labeled as "refrigerated noodles" or "plastic silverware," products that are unlikely to raise suspicion.[31] Other false documents may include stolen importer identities. Chinese criminal enterprises have stolen the identities of legitimate importers with no history of trafficking in infringing goods in order to increase the likelihood of their infringing goods clearing United States Customs. Other counterfeiters steal authentic business information to use for both export and import of infringing goods. The false shipping documents give the impression the goods being shipped are originating from a legitimate manufacturer and being sent to a legitimate distributor. The products, however, are redirected after clearing customs to be received by illegal distributors, not the legitimate business.[32] When Chinese criminal enterprises learn that Customs has "red-flagged" one of the enterprises' corporations as an importer of counterfeits, the enterprise will simply create a new corporation as the new importer of record to import the same counterfeit goods.

Figure 1: Domestic Value of IPR Seizures by Shipping Method (in millions)

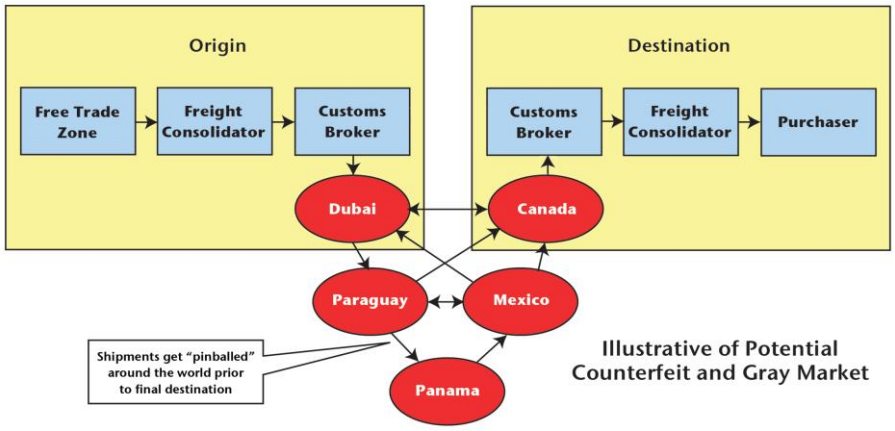


Source: U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, "Intellectual Property Rights Fiscal Year 2010 Seizure Statistics – Final Report," January 2011.

In addition to false shipping documentation, fraudulent certificates of authenticity or performance history may be included with the infringing goods in the container to attempt to disguise them as legitimate goods. For example, counterfeit aircraft parts may be shipped with illegally altered documents or forged certificates of authenticity.[33]

In an effort to draw less attention to containers of infringing goods, some distributors will ship the goods via other countries with a less negative reputation as a country of origin for infringing goods. This method is referred to as transshipping. For example, goods shipped from China may first travel to India or Singapore and then to the United States.[34] Some shippers will even offload the goods in the other country before reloading and shipping onward to completely disguise the fact that the goods actually originated in China.[35] Figure 2 depicts how containers of infringing goods may begin in one country, be shipped to several other countries, and eventually be distributed to consumers in the United States.[36]

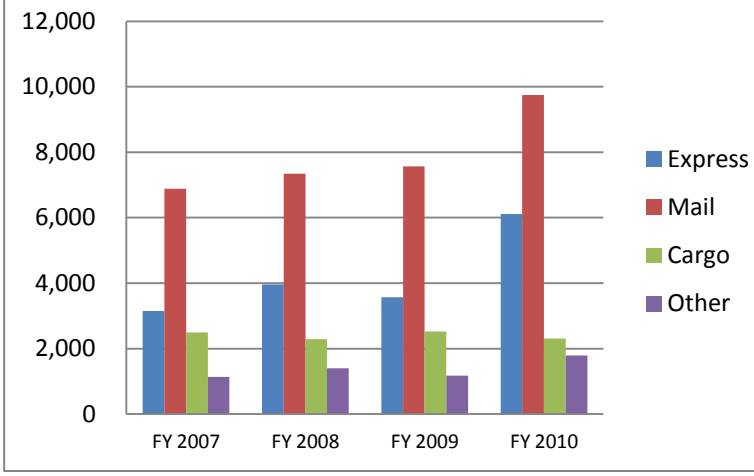
Figure 2: Transshipment of Infringing Goods



Source: Motor & Equipment Manufacturers Association Brand Protection Council, "Understanding the Flow of Counterfeit and Gray Market Goods through the U.S. Automotive and Commercial Vehicle Parts Marketplace," January 2009.

Current trends indicate IPR violators are using more discrete shipping methods to transport their goods. As depicted in Figure 3, significantly more IPR seizures are of goods shipped via postal and express consignment services in smaller packages containing fewer items instead of entire shipping containers stocked with infringing goods.[37] These smaller packages of infringing goods are believed by counterfeiters to decrease the likelihood of customs inspections and seizures. Moreover, if the contents are discovered and seized, the counterfeiter has lost significantly less product than losing an entire container's worth of goods. Counterfeit pharmaceuticals are often distributed to the United States using this method.[38]

Figure 3: Number of IPR Seizures by Shipping Method



Source: U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, "Intellectual Property Rights Fiscal Year 2010 Seizure Statistics – Final Report," January 2011.

Some evidence indicates criminal enterprises or organized crime groups in the United States travel to other countries to collect infringing goods and smuggle them into the United States for further distribution. For example, members of the Yi Ging Organization traveled to China, acquired illegal copies of American and Chinese DVDs, smuggled them into the United States, copied the DVDs, and distributed them with pirated music CDs to stores they controlled in New York City.[39]

The increased availability and use of the Internet has contributed to the dramatic growth of online piracy and facilitates the sale and distribution of physical infringing goods with little respect for geographical borders. Consumers of infringing goods are able to make purchases online, as well as take advantage of pirated multimedia content posted to the Internet. Counterfeit luxury goods and clothing are sold to United States consumers via websites. Infringing pharmaceuticals, particularly lifestyle drugs, are increasingly available for purchase via the Internet. The infringing goods will then be shipped directly from the manufacturer to the consumer. As ICE Director John Morton stated, "the Internet has just completely changed the face of the [IPR] problem, made it more complicated and more pervasive. Whole industries now have been attacked, not from the street, but from the Internet."[40]

In addition to individuals purchasing infringing goods via the Internet, United States companies and the United States military often purchase products, such as aircraft parts, automotive parts, and electronics, using the Internet. In some cases, the purchase of products by these organizations has resulted in the unintentional purchase of infringing goods. For example, the United States military purchased counterfeit microchips valued at $2.7 million from a broker working out of her home in California who simply purchased inexpensive chips from websites. The broker was later identified to have no formal education in microchips and many of the chips were discovered to be counterfeit.[41]

After infringing goods enter the United States they are distributed to domestic retailers and consumers. As these domestic distribution networks pertain specifically to the United States, they will be detailed in Section VII, E of this report.

3. Supply chain vulnerabilities

One of the areas of greatest concern from infringing goods is vulnerabilities in the legitimate supply chain.[*] Infringing goods in the legitimate supply chain are intended to deceive customers into believing they are buying genuine goods. Although some industries, such as luxury goods and pharmaceuticals, have little to no evidence of infringing goods entering the legitimate supply chain,[**] other industries, including aircraft parts, electronics, and automobile parts, have experienced breaches in their legitimate supply chains.[42]

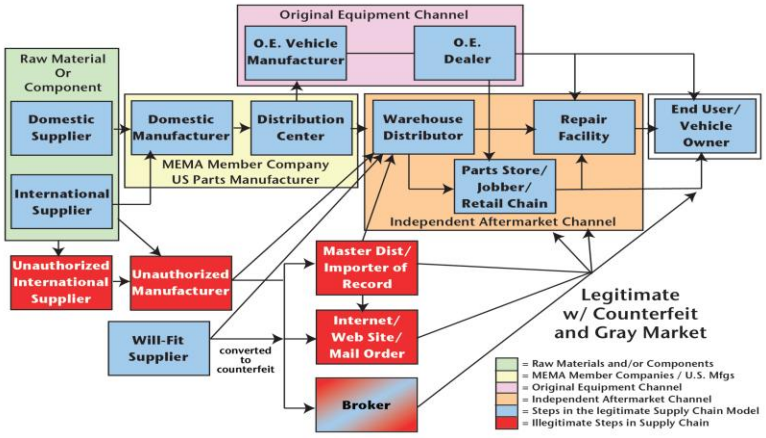
The industries with little to no infringing goods in the legitimate supply chain have extremely strict guidelines regarding the manufacturing, distribution, and sales of their products. Certain luxury goods companies only have their products manufactured in one location, shipped by one company, and sold in brand name stores affiliated with the company.[43] A tightly controlled supply chain means less vulnerability to be exploited and minimizes the chances of infringing goods entering the supply chain. For example, pharmaceuticals have very few wholesalers and the sales process is highly regulated to ensure that controlled substances are not provided to unlicensed operators.

[*] The legitimate supply chain includes authorized distributors of products.

[**] Although little evidence indicates infringing goods from these industries have entered the legitimate supply chain, significant evidence indicates there is an extensive secondary, illegitimate supply chain used to sell infringing goods. This illegitimate supply chain will be discussed in greater detail later in this section.

Legitimate supply chains in other industries, such as the automotive, electronics, and aircraft parts industries, are more frequently compromised because they have large, complicated distribution networks. As depicted in Figure 4,* numerous suppliers, manufacturers, and distributors may be involved in a single purchase of products.[44] As there is often little tracking of the shipment of products from the original manufacturer to the end user, there are countless vulnerabilities in the supply chain. Industry representatives for the automotive replacement parts and aircraft parts industries explained counterfeits often will be mixed into shipments with legitimate products in an effort to disguise the counterfeits.** If the end users randomly test some of the products, they may not select the counterfeit products, allowing the infringing goods to pass into the legitimate supply chain and be installed on final products.[45]

Figure 4: Automotive and Commercial Vehicle Parts Distribution Supply Chain Model



Source: Motor and Equipment Manufacturer's Association Brand Protection Council, "Understanding the Flow of Counterfeit and Gray Market Goods through the U.S. Automotive and Commercial Vehicle Parts Marketplace," January 2009.

Many infringing goods – such as luxury goods and multimedia content – are targeted to the secondary market and thus do not enter legitimate product supply chains. Consumers know or have reason to believe the products they are purchasing are counterfeit and accept the risks associated with these purchases. Counterfeit pharmaceuticals may also be distributed in the secondary market where consumers turn a blind eye to the risks. By bypassing legitimate supply chains the distributors of these infringing goods are undermining the regulations and protections offered by legitimate supply chains. For example, consumers purchasing pharmaceuticals from a local authorized pharmacy are reasonably assured the products they receive are legitimate and safe. However, consumers purchasing pharmaceuticals from an online pharmacy may be purchasing counterfeit pharmaceuticals that have not been tested for authenticity and have no guarantee of safety or effectiveness.

* Although this diagram is specific to the automotive industry, similar patterns were observed in the aircraft industry and Department of Defense supply chain.

** Industry representatives reported significant differences between infiltration of supply chains of parts to the Original Equipment Manufacturers (OEM) and replacement part supply chains. Due to the direct distribution of large quantities of parts from trusted suppliers to the OEMs, there is little evidence of infiltration of counterfeit goods to OEMs. Because the number of suppliers and customers increases significantly in the replacement parts business, it is much easier to insert infringing goods into the replacement parts supply chain.

V. THE MAGNITUDE OF THE THREAT

This portion of the analysis evaluates existing estimates of the magnitude of the threat to United States interests from IP theft. It also examines alternative measures and identifiable trends in specific aspects of the threat, including the global trade of counterfeit goods, the economic impact on rights holders and the United States government, health and safety ramifications, national security risks, and theft of trade secrets. This section also provides an overview of the magnitude of the threat in selected industries.

Accurately measuring the threat from IPR criminal violations is extremely challenging. Measurements may be affected by a multitude of complications, such as competing definitions of the threat, the types of infringing items being counted, the inability to accurately measure undiscovered activity, the lack of centralized data repositories, ambiguities in how violations are reported, and the varying types of harm and impacts caused by the violations. Assuming these factors could be addressed and quantified, accurate measurements would still require sophisticated econometric models to estimate the size of the unknown portion of the threat. As such, this analysis does not endeavor to generate new data regarding the size of the threat but instead focuses on existing measurement efforts.[*]

A. Dimensions of the Threat

The negative impacts from IP theft are multi-dimensional and extend beyond rights holders. As noted in Figure 5, consumers, the government, and the economy may all suffer consequences from these violations. No one measure of the threat can capture all of these dimensions.

Figure 5: Negative Effects of Counterfeiting and Piracy, by Stakeholder

Stakeholders	Negative Effects
Industries	Lost sales and brand value, increased IP protection costs
Consumers	Health and safety risks, low quality goods
United States government	Lost tax and customs revenue, increased enforcement costs, and risks to supply chains with national security (including risk to war fighters) or safety implications
United States economy	Lower growth and innovation, declining trade with countries having weak IP rights enforcement

Source: Government Accountability Office, "Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods," April 2010.

[*] However, there are two ongoing efforts within the United States government to develop more accurate estimates of elements of this threat. First, pursuant to the Intellectual Property Enforcement Coordinator's Strategic Plan, the Department of Commerce is leading an effort to measure the economic contribution of intellectual property intensive industries. Second, in response to a congressional request, the International Trade Commission (ITC) prepared an estimate of the impact of IPR violations originating in China. The ITC report was released May 18, 2011which was too late for its findings to be incorporated into this report. The ITC report can be found at http://www.usitc.gov/publications/332/pub4226.pdf.

The magnitude of the threat is driven by those who demand or purchase infringing goods, as well as those who supply them. Specific demand for counterfeit or pirated goods primarily originates in the secondary market from individuals who knowingly purchase counterfeit goods. These consumers wish to save money, are willing to receive goods that may not meet the standards of the genuine product, and/or do not perceive a significant risk from doing so. However, there may be some "demand" in the primary market from consumers who believe they are purchasing genuine goods but still want a bargain. In such cases, the infringing goods resemble genuine goods and the price differential is not so large as to clearly indicate the goods are counterfeit.

Certain industries exhibit larger consumer demand for infringing goods than others. The luxury goods and music and movie industries, for example, have large demand for infringing goods. In the case of luxury goods, such demand often is driven by individuals who wish to have the cachet of the brand name without the corresponding expense. Demand for pirated content may be driven either by the desire to obtain a bargain or by those who disagree with IPR protections. In contrast, other industries may exhibit lower demand for known counterfeit goods because technical performance is more important to consumer satisfaction and/or the purchasers are aware of potentially grave risks to consumers' health and safety and are not willing to take these risks. The aircraft replacement part industry is an example of such an industry. The pharmaceutical industry might be expected to have low demand because effectiveness is the essential reason for purchasing the item and there are significant health and safety risks from ingesting ineffective or tainted goods. The high demand for pharmaceutical products from websites offering counterfeit drugs suggests consumers are insufficiently educated as to the nature of the drugs they are purchasing, are unaware of the potential risks from counterfeit drugs, or are aware of and willing to accept the risk.[*]

1. Estimates of overall trade figures

Some efforts attempt to determine, on a macro level, the magnitude of the threat based on the international trade in infringing goods. The most notable of these are the estimates produced by the Organisation for Economic Co-Operation and Development (OECD) in 2008 and 2009.[46] OECD estimated counterfeit or physical pirated goods accounted for 1.95 percent of all 2007 world trade.[**47] The OECD estimates did not include domestically produced and consumed goods or digital piracy. It conceded, however, "the overall degree to which products are being counterfeited and pirated is unknown, and there do not appear to be any methodologies that could be employed to develop an acceptable overall estimate."[48] OECD further conceded its estimates are merely a general indicator of the size of the threat as opposed to a refined calculation. These calculations involve assumptions that may or may not be accurate and do not

[*] For example, one industry representative spoke of an individual who ordered drugs over the Internet and contacted the maker of genuine goods to ask why the drugs did not look like others he had purchased before – these were a different color and arrived in a plastic bag. When told he had purchased counterfeit drugs he asked the company to test them for him to determine what they were. When told the company does not test drugs for consumers, the individual indicated he would take the medication and see if it worked.

[**] In contrast, in 2004 the International Chamber of Commerce (ICC) Counterfeiting Intelligence Bureau estimated in that infringing goods constituted 5 to 7 percent of international trade. See ICC Counterfeiting Intelligence Bureau, "The International Anti-Counterfeiting Directory 2009," 2009, 11, http://www.icc-ccs.org/images/stories/pdfs/iacd%2009.pdf.

account for varying rates of infringement across different industries. Regardless, these estimates suggest the threat is very large and growing rapidly.

Figure 6: Estimates of International Trade in Infringing Goods (in billions)

	2005 (OECD)	2007 (OECD)	2008 (BASCAP)	2015 (Est.) (BASCAP)
Value of infringing goods traveling across borders	$200	$250	$285-360	$770-960
Domestically produced and consumed infringing goods	N/A	N/A	$140-215	$370-570
Digital piracy	N/A	N/A	$35-70	$80-240
Total	N/A	N/A	$460-645	$1,220-1,770

Source: Organisation for Economic Co-Operation and Development, "The Economic Impact of Counterfeiting and Piracy," 2008; Frontier Economics, "Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report Commissioned by the Business Action to Stop Counterfeiting and Piracy (BASCAP)," Feb. 2011.

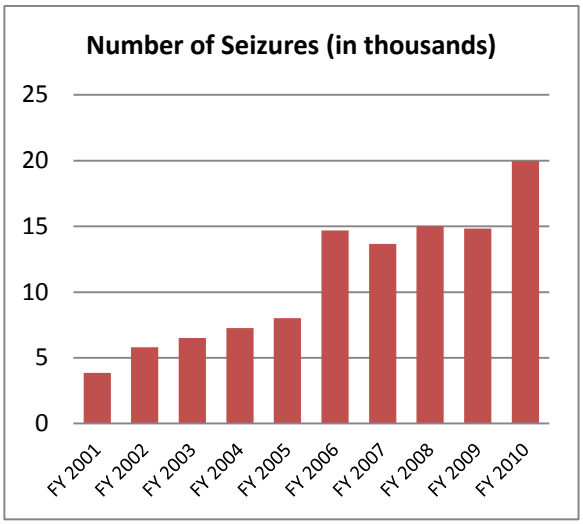
A recent report commissioned by the International Chamber of Commerce's Business Action to Stop Counterfeiting and Piracy (BASCAP) initiative updated the OECD estimates using 2008 data.[49] This study also provided estimates for two categories the OECD figures ignored – domestically produced and consumed infringing goods and any digitally pirated products.[50] It argued that because of the rapid increase in infringing goods between 2005 and 2008, these figures probably underestimate the level of counterfeiting and piracy beyond 2008.[51] Based on the assumption that current growth rates in counterfeiting and piracy were to continue, BASCAP estimated the amount of counterfeiting in 2015 would be measured in the trillions. As these figures are based on the same methodology that OECD concedes produces merely general indicators, BASCAP's figures should also be viewed as providing general indicators as opposed to precise figures.

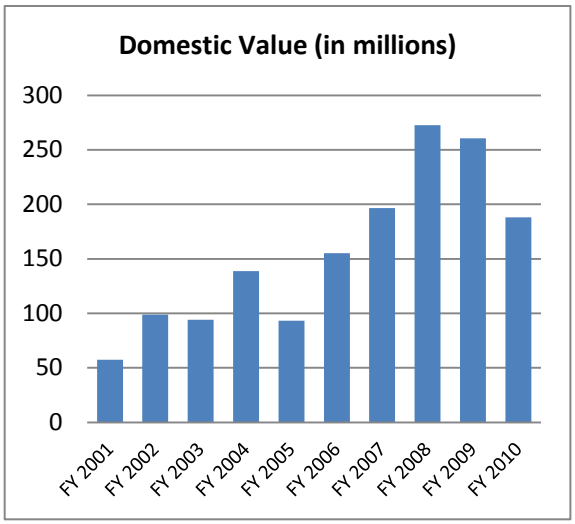
Even without a concrete measurement of overall infringement, there are some notable trends. First, regardless of the measure used, every report indicates the problem is growing. The OECD figures indicate a 25 percent increase in just two years. The BASCAP study reports between 2005 and 2008 there was an annual increase of 22 percent in the international trade value of counterfeited and physically pirated goods.[52] It estimates that from 2008 to 2015 the amount of infringing goods will increase over 240 percent. [53] One analysis reported worldwide production of counterfeit goods has jumped 1,700 percent since 1993.[54]

Yearly seizures by CBP and ICE have been trending upward since 2001. The number of seizures increased 83 percent from 2005 to 2006 and 43 percent from 2009 to 2010. These higher levels of seizures are due to increases of seizures at mail and express package centers.[55] Seizures in

2010 had a domestic value* of over $188 million.** The estimated manufacturer's suggested retail price for these goods, if they had been genuine, was $1.4 billion.[56]

Figure 7: United States IPR Seizures (Number and Domestic Value)

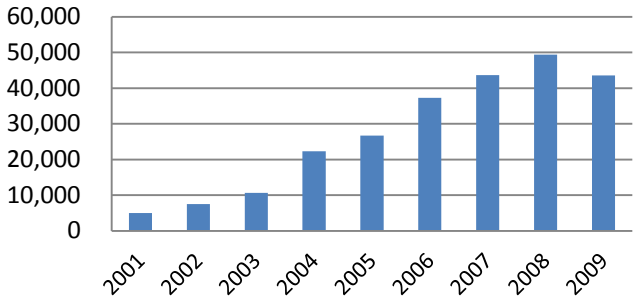




Source: U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, "Intellectual Property Rights Fiscal Year 2010 Seizure Statistics – Final Report," January 2011.

It is impossible to know what percentage of counterfeit goods arriving at United States ports is seized, but seizures are believed to significantly under represent the amount of counterfeit goods crossing the border. Although some of the observed increases in seizures may be due to more or better directed resources, this continual and dramatic increase in seizures at a rate above the growth in imports is an indicator of the increasing threat of infringing goods from overseas. As depicted in Figure 8, the European Union reported similar trends.[57] Based on an assumption that rising seizures reflect more infringing goods, the BASCAP study concludes

Figure 8: European Union IPR Seizures



Source: European Commission – Taxation and Customs Union, European Commission Report, Executive Summary, "Report on EU Customs Enforcement of Intellectual Property Rights: Results at the EU Border – 2009."

* Domestic value is the "price for which a seized or similar property is freely offered for sale at the time and place of appraisement and in the ordinary course of trade." 19 C.F.R. 162.43(a). There is a significant difference between the value based on the manufacturer's suggested retail price for these goods and the domestic value. For example, in August 2009 CBP reported seizing 1,226 cartons of wearing apparel with a manufacturer's suggested retail price of $3.9 million but an estimated domestic value of $400,000. In January 2010 it seized 252,968 DVDs with a suggested retail price of more than $7.1 million, but it estimated the domestic value as $204,904.

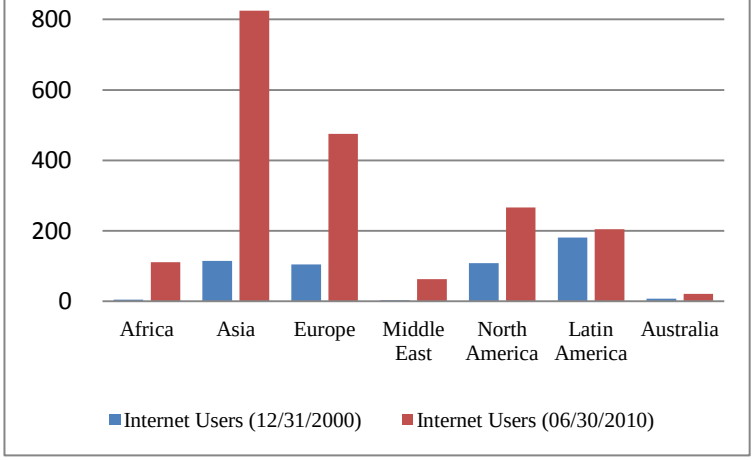
** Although the actual number of seizures increased in 2010, the domestic value declined 28 percent. CBP attributes this trend to an increase in seizures of lower value express consignment/mail seizures, which is consistent with the shift in how counterfeiters are moving goods across borders.

these additional seizures reflect an additional $37.5 to $112.5 billion of globally traded infringing physical goods.[58] As additional seizures may mean better enforcement as well as more infringing goods, the BASCAP assumption may overstate the amount of the increase in infringing goods.

At the same time the breadth of the types of products being counterfeited has expanded.[59] There are "virtually no product lines, corporations, or consumers that escape the reach of counterfeiters and/or pirates."[60] Products currently known to be counterfeited include pharmaceuticals, auto parts, hand tools, shampoos, foods, razor blades, airplane parts, light bulbs, film, skin lotions, laundry detergent, adhesive bandages, insecticides, batteries, and cigarettes.[61] The ability to make appearingly perfect copies was enhanced with digital technology. The products and high quality packaging may appear so genuine that only scientific testing can distinguish between original and imitation.[62]

The increasing use of the Internet to sell and purchase goods also broadened the market for infringing goods. Historically, distribution of counterfeit goods "was confined to fly-by-night networks, street-corner vendors, street stalls, etc., with no real organization. This distribution model limited the market penetration of counterfeit goods."[63] In contrast, the Internet permits counterfeiters to reach an increasing pool of buyers around the world and around the clock. As depicted in Figure 9, worldwide Internet usage grew 444.8 percent from 2000 to 2010. Over 77 percent of the North American population used the Internet in 2010.[64] Although the penetration percentage figures are smaller for Europe and Asia, the actual numbers dwarf the North American numbers. China alone has an estimated 420 million users.[65] The amount of wired broadband subscriptions worldwide was estimated to be 555 million by the end of last year.[66] Many of these users will use the Internet to make purchases. A Nielsen Company survey in 2008 reported "over 85 percent of the world's online population has used the Internet to make a purchase, up 40 percent from two years ago, and more than half of Internet users are regular online shoppers, making online purchases at least once a month."[67]

Figure 9: Number of Internet Users 2000, 2010



Source: Internet World Stats, "Internet Usage Statistics – The Internet Big Picture, Internet Users and Population Stats."

The expansion of Internet use is a critical factor in the dramatic increase in online piracy. Online piracy currently accounts for between 6.5 and 12 percent of the total value of infringing goods.[68] Due to technological improvements that make online piracy easier, such as rapidly increasing Internet access and faster broadband speeds that facilitate greater illegal downloading and file sharing, BASCAP estimates the value of online piracy could reach $240 billion by 2015.[69]

There is a continuing shift from the lower-profit secondary market – where goods are sold at a significant discount compared to the genuine product – to the higher profit primary market – where purchasers are willing to pay higher prices because they believe they are receiving the genuine product.[70] As a result there are, at least in appearance, higher quality infringing goods in the marketplace and consumers are more likely being deceived. Without accurate information regarding the goods they are purchasing, they may be more likely to unknowingly incur an increased risk to their health and safety. Increased use of the Internet is making it easier for infringers simultaneously to reach – and segment – both the primary and secondary markets.

2. Measuring the impact on rights holders

These general trade figures do not measure the different dimensions of harm across the spectrum of stakeholders. The first such gap is any measure of the economic impact of IP theft on the rights holders. The OECD and BASCAP figures measure the value of the infringing goods but do not attempt to estimate the business losses resulting from the sale of these goods. Estimating losses is difficult because it requires measuring the rate at which purchasers of an infringing good would purchase the genuine good if the infringing good was not available; this figure varies significantly across countries and industries.[71] Measuring losses is also complicated by the inability to measure the amount of infringing goods that have not been identified or seized and the lack of a uniform measure of value to the rights holder (e.g. the suggested retail price, the average price received for the product, or the incremental profit the rights holder would have received if it had sold the goods).

The copyright industries have provided estimates of actual losses to their rights holders. The Institute for Policy Innovation (IPI), supported by the Recording Industry Association of America (RIAA), estimated a global loss of $6.37 billion to United States music industry producers and retailers due to all forms of piracy.[72] The Motion Picture Association (MPA) estimated the United States motion picture industry lost nearly $6.1 billion worldwide in 2005.[73] The accuracy of these figures is highly dependent on the accuracy of assumptions regarding the rate of substitution and the price legitimate purchasers would have paid. These figures may also have been influenced by the fact they were produced on behalf of industry representatives who may benefit most from larger loss estimates.

In addition to lost sales, there are collateral consequences, such as damage to brand value by dilution (a flood of inexpensive counterfeit luxury goods will make the brand less exclusive and therefore the premium paid for exclusivity will diminish) or declining reputation (defective or dangerous counterfeits may confuse consumers and cause them to not purchase the same brand because they do not believe it provides quality). Rights holders also must expend costs to protect their rights.

None of the studies estimating the impact of infringement on the rights holders attempt to measure any of these consequences, yet they may be significant.[74] For example, brand protection is critical to many companies. Companies may be defined by their reputations and "[a] good reputation and a strong brand allow companies to stand out in crowded markets."[75] One expert argues up to 40 percent of a company's value can be tied to its reputation.[76] The value of the brand name for leading companies such as Coca-Cola, Microsoft, Intel, and Disney

are in the billions of dollars. Nine of the ten top brand holders in the world are United States companies.[77] As one expert noted, it can take 20 years to build a reputation but only five minutes to ruin it.[78] Counterfeiters in the primary market may operate anonymously and have no reputation to protect or liability concerns.[79] As a result, legitimate brand holders' reputations may be at the mercy of unscrupulous operators. If poor quality or (even worse) dangerous counterfeits are found in legitimate sales outlets, there could be a significant backlash against the brand owner.[80] Some companies are afraid to acknowledge counterfeits of their products exist because consumers may switch to a competitor's brand that has not been linked to counterfeiting.

Protecting one's brand is one of the top ten principles of a strong brand.[81] As a result, rights holders told IPR Center personnel they are expending increasingly more resources to protect against counterfeits. One interviewee reported beginning his career in the company doing forensics on products that malfunctioned. It was not until later, after someone brought to the company's attention that its trademark was being counterfeited, that it built an anti-counterfeiting unit. This unit now has personnel stationed around the world conducting investigations and working with law enforcement to protect against counterfeiters. This individual reported CBP made 330 seizures of goods with counterfeit versions of the company's trademarks in 2010 – the equivalent of almost one a day. The company has created expensive holographic labels using special ink brought in by armored vehicle. The company serializes the labels and controls the quantities to ensure manufacturers only received one label per legitimate product.[82]

This is just one example of the tremendous cost companies expend to protect their brand against counterfeiters. Virtually every rights holder representative interviewed for this analysis was employed in a portion of his or her company that addresses counterfeiting and/or piracy issues. Although there are no estimates of the total cost brand owners spend annually on anti-counterfeiting efforts, interviews of rights holders indicate these efforts are significant and increasing exponentially.

3. Measuring the health and safety impact

Numerous industries produce products which, if counterfeited, pose potential health and safety concerns to the United States public. Pharmaceuticals, automotive parts, aviation parts, electrical components, medical devices, personal care products, and even food can be counterfeited and pose a potential health and safety risk to the United States public.

There has not been a systematic analysis of the magnitude of the health and safety risk to United States interests from infringing goods. Interviewees consistently informed the IPR Center that linking particular deaths, illnesses, or injuries to counterfeit goods is extremely difficult. When an already ill patient dies, it is unlikely a medical professional will examine the patient's medicine to determine whether it is genuine or counterfeit. Similarly, when a fire breaks out from faulty electric cords or circuit breakers the fire may consume the evidence.

The BASCAP study is the only attempt to estimate these potential health and safety costs the IPR Center found. This study, however, suffers from a lack of supporting evidence. The BASCAP study estimated counterfeiting costs the G20 economies $18.1 billion per year due to deaths.[83] This figure is based on 3,000 consumer deaths per year worldwide from exposure to counterfeit

products, mostly counterfeit food and medicines.[84] This study does not indicate the source of the number of deaths and BASCAP has previously acknowledged governments "collected only limited data on deaths associated with counterfeiting."[85] It is therefore impossible to determine which countries reported these deaths or evaluate the conclusion that they were due to counterfeit goods.

This same study estimated an additional $125 million in annual costs for health services to treat injuries caused by dangerous counterfeits.[86] There is no indication as to the basis for this figure as the report concedes there "are few good sources of information" on accidents and other negative health effects from counterfeiting.[87] There is also no information as to where or how these injuries occurred. Although this figure may in fact be a reasonable estimate or even underestimate the true economic costs of the health and safety impacts of poor quality counterfeit goods, there are no means for determining the reliability of the figure.

Operations directed specifically at these types of products result in significant seizures. For example, between July and September 2010, ICE-HSI, CBP, and the Mexican Revenue Service seized a variety of infringing goods posing potential threats to the public's health and safety, including counterfeit electronic products, pharmaceuticals, critical components (i.e. networking software), automobile airbags, rifle sites, Airsoft guns, cellular phones, batteries and chargers, and health and beauty products.[88] As a result of this one operation, infringing goods valued at more than $23 million were seized at express courier consignment and international mail facilities in the United States, and over 300 tons of counterfeit goods were seized in Mexico.[89] Although not a representation of the total number of infringing goods posing potential health and safety threats in the United States, the figures nevertheless indicate a significant problem.

CBP and ICE report annual seizure statistics for counterfeit products that pose potential health and safety concerns but do not test all products to determine the extent of the actual danger. In addition, variations in the amount of these goods seized in a given year may unfairly skew the perception of risk. For example, in 2008 the domestic value of pharmaceutical seizures increased 152 percent over the prior year's amount. One should not conclude from this statistic that the risk from counterfeit pharmaceuticals was 152 percent greater than the prior year, or conversely that the risk was significantly lower in the surrounding years. In 2008, CBP conducted a large initiative aimed at counterfeit pharmaceuticals, which is the likely cause of the large increase in seizures. In 2009, after the initiative's conclusion, seizures of pharmaceuticals fell back to within one percent of the 2007 figures.[90] Furthermore, as counterfeit pharmaceuticals are increasingly shipped in smaller quantities by mail, the number of pharmaceutical seizures increased while the value of the overall seizures declined.[91]

Although there is no accurate way to measure the overall magnitude of the health and safety threat, it is reasonable to conclude the threat is serious. For example, the Consumer Product Safety Commission issued several recalls for hundreds of thousands of circuit breakers with the Square D trademark on them because counterfeit breakers that could fail to trip when overloaded and cause fires had made their way into the legitimate supply chain and were being installed in homes and businesses.[92] Counterfeit automotive parts can be dangerous as counterfeit "suspension parts and wheels break when made of substandard material; vehicle hoods without crumple zones penetrate the passenger compartment; counterfeit brake pads made of grass

clippings and saw dust have caused fatal accidents; and counterfeit windshields without safety shatterproof glass cause injury or death."[93] A World Customs Organization review of potentially dangerous counterfeit items seized in 2004 included over "1 million counterfeit Viagra tablets, approximately 151,000 automobile parts of variable quality and often containing counterfeit versions of automobile safety features, parts for boats and trains, and even a part for the landing gear of a Boeing 747 aircraft."[94]

4. Measuring the global economic impact

In addition to the economic impact on rights holders, the rapid increase in infringing goods has an impact on the global economy – including replacing legitimate economic activity, lowering tax revenues, losing customs duties, and displacing legitimate jobs producing and distributing genuine goods.[95] The BASCAP study endeavored to measure several categories of economic harm, including lost tax revenues, lost legitimate employment, the increased costs of crime, and the economic costs of the injuries to consumer health and safety for the G20 countries. Unfortunately, these figures do not appear supported by reliable evidence and likely overstate certain cost elements. The BASCAP study estimated these additional consequences of IP theft cost the G20 governments and consumers over $125 billion each year. This figure includes approximately $77.5 billion in lost tax revenues and higher welfare spending, $25 billion in increased costs due to crime, $18.1 billion in economic costs from deaths resulting from bad counterfeit products,[*] and an additional $125 million for health related costs for treating injuries as a result of dangerous fake products. The study also estimated approximately 2.5 million legitimate jobs have been lost due to counterfeiting and piracy.[96]

There are no means for measuring the reliability of the BASCAP estimates because it is not possible to determine the validity of the underlying assumptions or the strength of the linkages between counterfeit goods and these specific economic measures. It is reasonable to conclude, however, that these types of losses occur and that they are significant.

5. Measuring the national security threat

IPR violations pose three significant potential threats to the national security of the United States.[**] The first is the unintentional use of counterfeit parts or pirated software on United States government or defense systems. These parts may malfunction and prevent government entities from effectively operating or communicating, or they may allow for potential security breaches from opportunistic offenders, such as hackers. The second is the deliberate insertion of malware or spyware onto counterfeit parts or pirated software with the intent of selling them to or installing them on sensitive United States government systems to allow foreign governments or enemies of the United States to spy on sensitive United States activities and communications. The third threat is economic espionage, in which foreign governments benefit from the theft of trade secrets of United States companies.

[*] Elsewhere in the report BASCAP contends there were 3,000 deaths a year due to counterfeit goods. If the economic loss from such deaths was $18.1 billion, then each death on average caused over $6 million in losses. That would appear unlikely.

[**] For the purposes of this report, the national security of the United States refers to the safety and well-being of United States government systems and operations, including those of the war fighters.

The most common threat appears to be the unintentional one. Although distributors of counterfeit parts may demonstrate disregard for the possible consequences of providing counterfeit parts to their customers, they are more likely driven by greed versus malicious intent. Moreover, because the DOD supply chain is so complex and numerous parts are interchangeable between systems, in many cases it would be virtually impossible for a manufacturer to predict which parts will be purchased and used by the United States government or where in the government a particular part might be used. Although it is clearer where parts that are specific to particular United States military equipment will be used, such as the B52 bomber or a missile, it still appears providers of counterfeit parts for these items are motivated solely by profit.

Pirated works that contain spyware and malware also may create unintended vulnerabilities in government systems. Again, the providers may not know which systems their products will be used on and so would have difficulty targeting particular systems. The key exception to this trend is where attackers direct phishing techniques at users of certain government systems to induce them into downloading software capable of opening back doors to the systems.

The economic espionage threat involves the misappropriation of a trade secret to knowingly benefit a foreign government, foreign instrumentality, or foreign agent. The size of this threat is difficult to measure because of the challenge of detecting the link between the trade secret theft and a foreign government or its agent. Since the passage of the Economic Espionage Act of 1996 there have been only seven economic espionage indictments. There have been, however, theft of trade secrets investigations and indictments with a foreign nexus.

One of the most thorough analyses of the magnitude of the threat from infringing goods to the United States national security is the January 2010 United States Department of Commerce (Commerce) assessment focusing on counterfeit[*] electronics in the DOD supply chain.[97] The Commerce assessment discovered counterfeit parts in all elements of the defense and industrial supply chain.[98] These infringing electronic parts, such as counterfeit integrated circuits,[**] "can result in product or system failure or malfunction, and can result in costly system repairs, property damage, and serious bodily injury, including death."[99] The Commerce report suggests the potential for the threat to the United States national security from malfunctioning or substandard infringing goods is significant.

Supply chains for replacement parts purchased by the United States government are vulnerable to infiltration of counterfeit parts. Military equipment often is required to remain in active duty longer than originally planned, causing a shortage of replacement parts.[100] This shortage can result in the government reaching outside traditional approved channels to a less controlled supply chain to purchase replacement parts.[101]

[*] In the Commerce study the term "counterfeit" includes both confirmed and suspected counterfeit parts as some companies were unable to perform the tests required to confirm a part is truly counterfeit.

[**] Integrated circuits are high-tech devices that control the flow of electricity. They are used in consumer electronics, transportation systems, medical equipment, spacecraft technology, and military equipment. See Department of Justice, "Owner and Employee of Florida-based Company Indicted in Connection with Sales of Counterfeit High Tech Devices Destined to the U.S. Military and Other Industries," *Press Release*, 14 Sept. 2010.

Suppliers outside the traditional supply channels frequently are not adequately vetted. Thirty percent of the counterfeit parts identified in the Commerce assessment came from parts brokers, the largest single type of source. Yet 98 percent of the 10,000 brokers in one database of brokers had fewer than 10 employees and had no quality control procedures in place.[102] As one industry organization noted, "All someone needs is a phone, a fax, and email address and they are in business."[103] For example, one supplier worked in her kitchen purchasing items via the Internet and subsequently sold these parts to the military. The individual had no expertise in the products she purchased and many were counterfeit. Another supplier's website displayed a picture labeled as the company's office, but further investigation indicated the company was based in the garage of the owner's house.[104] A Naval Air Warfare Systems Command (NAVAIR) researcher estimated 15 percent of all spare and replacement microchips the United States military buys are counterfeit, including older parts with inaccurate dates made to appear newer or commercial grade products relabeled as military grade.[105]

These cases may involve large numbers of parts. For example, in September 2010 two individuals in Florida were indicted for selling to the United States Navy, defense contractors, and others, over 59,000 counterfeit lower grade integrated circuits from China and Hong Kong falsely labeled as "military-grade."[106] In a similar example, a United States citizen and his relatives imported over 13,000 counterfeit integrated circuits from China, re-marked them with infringing trademarks, labeled them "military grade," and sold them to the United States Navy.[107] A series of investigations of counterfeit products bought by government agencies and contractors as of May 2010 had uncovered over 94,000 counterfeit Cisco Systems network components.[108]

Legitimate supply chains also may be infiltrated by pirated software that governments or government contractors may purchase unknowingly. There are at least two reports of state and local governments purchasing computers preloaded with pirated software from apparently legitimate vendors. The purchasers were unaware the software was counterfeit. In these cases the vendors loaded the software prior to selling the computers. The pirated software prevented the owners from receiving the updates needed to protect them from cyber attacks and left the computers vulnerable to computer intrusions. In both cases it appeared the vendors only wanted to increase their profit margins, but the potential consequences to the government systems that contained sensitive information could have been devastating.[109]

The number of infringing goods installed on DOD systems is unknown. The Commerce report explained the most common methods for companies discovering counterfeits were parts returned as defective and the discovery of parts as poor performing. The report did not indicate how many of these parts were discovered as defective or underperforming during testing as opposed to after installation.

Infringing products have compromised United States government agencies' computers. Melissa E. Hathaway, former head of cyber security in the Office of the Director of National Intelligence, publicly revealed "counterfeit products have been linked to the crash of mission-critical networks, and may also contain hidden 'back doors' enabling network security to be bypassed and sensitive data accessed [by hackers, thieves, and spies]."[110] In one such incident a user with administrative privileges installed Peer-to-Peer software (P2P) on an unclassified government

computer. The user downloaded a copy of pirated software that included a backdoor Trojan.* The Trojan had the capability to allow a remote attacker to acquire system information, exploit and replicate itself on network systems, download and upload files, and access the computer remotely. A keylogger** was installed and executed on the government computer.[111] Although there is currently no indication foreign governments are using counterfeit goods to access United States government systems, several foreign governments may be capable of exploiting such goods in this manner.[112]

Particular types of counterfeit goods on government systems could create vulnerabilities to espionage. The majority of the counterfeit parts found in the DOD supply chain originated in China.[113] The majority of cyber attacks against DOD and United States civilian agency systems are suspected to have originated in China.[114] Although these hackers use intrusion techniques, not IPR violations, the presence of counterfeit parts or pirated software on sensitive United States systems could make the systems more vulnerable to such attacks. As such, it is possible Chinese offenders could seek to install counterfeit products onto United States government systems to facilitate easier network exploitation.

In addition to causing harm to sensitive United States systems, counterfeit products can also threaten the safety of United States war fighters. For example, a man was found guilty in 2010 of trafficking in counterfeit Cisco products. The offender purchased counterfeit Cisco Gigabit Interface Converters (GBICs) from a vendor in China with the intention of selling the parts to DOD for use by the United States Marine Corps. The GBICs were going to be installed on computer networks used to transmit troop movements, relay intelligence, and maintain security for a military base in Iraq.[115]

6. Measuring thefts of trade secrets

Trade secrets encompass a wide array of critical information ranging from how highly technical products are engineered to how to manufacture items to customer data. This threat is multi-dimensional and encompasses potential economic loss to rights holders, the potential loss of critical United States technological advantages, and possible threats to national security if information taken from civilian industries is converted for defense or other sensitive applications.[116]

The IPR Center did not find any estimates of the magnitude of the threat from thefts of trade secrets. The only known measure is the number of cases charging this type of violation. From 2002 through 2010 federal law enforcement prosecuted hundreds of theft of trade secrets cases. It is likely the number of prosecuted cases underestimates the size of the actual threat.

The types of information targeted in these thefts were broad, ranging from pharmaceutical formulas to source code to microwave technology to paint formulas. There does not appear to be a consistent pattern as to the types of information targeted. There has not been a systematic

* A Trojan is a destructive program that masquerades as a benign application.

** A keylogger is a type of surveillance software that is capable of recording every keystroke a user makes to a log file. It can record any information typed on a keyboard, including usernames, passwords, emails, and may even capture encryption keys.

analysis of the economic losses from these cases, but they are often very large with some cases reporting economic losses in the hundreds of millions or even billions of dollars.[*]

7. Industry Specific Estimates

Multimedia content

This section is focused on piracy of music, movies, and business software. The threat from music and movie piracy is primarily an economic one, with losses to rights holders as well as broader economic losses from lost tax revenues and lost jobs. As noted previously, pirated software also poses a significant security threat to computers and their networks.

One analysis supported by the music industry estimated a global loss of $5.33 billion to United States music industry producers from all forms of piracy. Approximately $1.630 billion was from physical piracy, while the remaining $3.703 billion was from online piracy.[**][117] Although the IPR Center cannot assess the accuracy of these specific loss figures, more objective figures such as sales, hits on piracy websites, and seizures substantiate that the threat is large.

Music industry revenue has fallen by half in the last ten years, from a record high of $14.6 billion in 1999 to $7.7 billion in 2009.[118] One estimate suggests 25 percent of the decline in music sales is due to piracy.[***] It was estimated that in 2010 approximately 40 billion songs were illegally downloaded worldwide, with 10-20 billion of them in the United States.[119] RIAA estimates only 37 percent of all music obtained in the United States in 2009 was obtained legitimately.[120] Industry reports 2.4 to 2.5 million infringing discs were seized in the United States in 2010. Online piracy increased exponentially in the second half of the last decade with the increasing availability of digital music.[****][121] In 2010, the music industry secured the removal of more than seven million infringing links.[122] There were also approximately 2,000 music piracy arrests in 2010.[123]

Industry officials believe the majority of the music that college and high school aged individuals possess was obtained illegally. They also estimated 50 percent of college students at some point

[*] For example, an August 2007 ASIS international survey reports survey respondents were unable to provide enough data about estimated losses to make any significant judgments. See ASIS, "Trends in Proprietary Information Loss," *International Survey Report*, Aug. 2007.

[**] The global value of digitally pirated recorded music was between $17 and $40 billion in 2008 but is more likely to be towards the upper end of this range.

[***] The amount of loss attributed to piracy versus other causes such as less money to spend on music, fewer big hits, etc. depends on the substitution rate used. How many of the individuals who obtained pirated content would purchase legitimate content if the pirated content was not available? The rates vary by type of pirating. It is estimated that more of the buyers of physical content (because they actually paid for the content just not to legitimate sources) would shift to legitimate sources than those who currently download music for free. The actual rate of substitution is contested but an estimate concluding that 25 percent of the loss in sales is due to piracy would appear to be at the conservative end.

[****] In 2004 fewer than 60 licensed music services operated online with only 1 million tracks available for purchase. By 2010 over 400 licensed music services existed online with 13 million tracks available for purchase. See IFPI Digital Music Report 2011, "Music at the touch of a button," 13.

engage in P2P downloading.[*] Approximately 20 percent of online users are believed to download content illegally at least once a year. In a survey of people who digitally pirated music, one individual who was asked what it would take for him to stop illegally downloading music allegedly replied, "You'd have to kill me."[124]

Although the primary impact of pirated music is economic, there is evidence of additional threats from malware introduced onto individuals' computers from downloaded pirated music. Although there is no known analysis of the overall size of this threat, one security company maintains a searchable database of viruses known to be associated with particular music piracy networks or websites and estimates that from 2009 to 2010 there was a 40 percent increase in websites posing a cyber threat to users' computers.[125] The use of P2P networks to download music also exposes the contents of the user's computer to others.

The Motion Picture Association (MPA) estimates the United States motion picture industry lost nearly $6.1 billion worldwide in 2005 due to piracy.[126] The IPR Center did not endeavor to verify this estimate but there is evidence such piracy is having an impact. Although worldwide box office revenues grew every year from 2006 through 2010 (due to a large growth of middle class moviegoers in countries such as China, Russia, and India), DVD sales of United States movies dropped 28 percent from their peak in 2004 through 2009.[127] This decline is believed to be due primarily to piracy.[128] As DVDs were estimated to generate 70 percent of film profits in 2009, a shift from legitimate DVD sales to pirated copies may have a significant impact on the industry.[**129]

In 2005, approximately 62 percent of infringing movie products were hard goods, while the remaining 38 percent were instances of digital piracy.[130] More recent analyses have found significant shifts to digital piracy.[131] In 2010, there were a reported 92.5 million illegal downloads of the top ten pirated movies.[***132] There are no comparable figures for the amount of streaming of these same films but industry experts believe the numbers are much higher. Illegal DVD sales have not disappeared completely. Sales still occur in street markets, or more recently, in box sets purchased via the Internet and drop shipped from China.[133]

Industry estimates 90 percent of piracy of newly released movies is traceable to individuals using digital recording devices in the theater to capture the images and sound.[134] Individuals used to record movies during regular showings, which would include heads of other audience members in the picture. Now individuals record films after hours when the theater is closed, allowing them to zoom in on the screen and use direct source sound to produce high quality copies.[135]

---

[*] Industry representatives noted they are watching closely what happens to these figure during the current academic year with the June 2010 passage of the Higher Education Act. That law has provisions requiring colleges and universities to monitor and prevent illegal content on their networks. It remains to be seen whether students will circumvent these restrictions by going off campus to locations with wireless networks or use mobile phone piracy.

[**] Legitimate streaming video on demand has greatly increased since this statistic was reported, therefore it is likely DVD sales no longer comprise such a high portion of film profits. However, digital piracy will likely compete with legitimate streaming video on demand, preventing the negative impact on the movie industry's revenue from abating.

[***] The number three film for illegal downloads, *Inception*, with a reported 9.7 million downloads, was notable because these downloads preceded the film's legitimate DVD release date. These figures were gathered by various groups that monitor BitTorrent sites and the IPR Center is unable to evaluate the validity of the figures.

Business software also experienced high piracy rates. The Business Software Alliance (BSA) estimated the value of unlicensed software worldwide in 2009 was $51.4 billion.*[136] The same survey concluded that in 2009 the global personal computer software piracy rate was 43 percent, a two percent increase from the prior year. The total value of the unlicensed software installed dropped slightly over the same period. [137]

The United States has a relatively low business software piracy rate – 20 percent – but because of the size of the domestic technology market, the United States had the single highest commercial value for unlicensed software in the world – over $8 billion. China came in second on a value basis, accounting for $7.6 billion of the value of unlicensed software. Twenty-three countries have piracy rates of at least 75 percent.[138]

Over 60 percent of business software infringement is "enterprise end-user software piracy." Such piracy occurs when someone in a business or government agency uses software without paying for it. For example, an organization may purchase one copy of software, either legitimate or pirated, but install it on multiple computers. Computer dealers or manufacturers may install unlicensed or pirated copies of software onto the computers they sell.[139]

Pirates also produce hard copies of software, often by criminal enterprises operating sophisticated factories that produce high quality copies with holograms and certificates of authenticity to deceive purchasers into believing they have purchased legitimate copies. These are often distributed via auction sites where pirated software distributors ship hard copies of software. Many of these sites are China-based business-to-business websites that usually offer products in bulk. The pirates ship the goods via legitimate shipping firms and use money orders or PayPal for payment.[140]

Beginning in 2005 the FBI and People's Republic of China's Ministry of Public Service (MPS) conducted a joint investigation into counterfeit software being produced in China and distributed around the world, including the United States. Seizures in China included over 290,000 counterfeit software CDs and certificates of authenticity. The software had an estimated retail value of $500 million. Seizures in the United States at distributors of products from the Chinese enterprises recovered approximately $2 million worth of counterfeit software.[141]

Although there are no figures indicating the relative size of digital piracy for business software, evidence indicates it is widespread and growing. In addition to seeing pirated software distributed via one-click file hosting sites, BitTorrent indexing sites, P2P distribution, and business to consumer (B2C) websites, industry noted an increase in warez community involvement in digital distribution of business software.[142] BSA reports that in the first half of 2009 it issued almost 2.4 million takedowns notices for pirated software file sharing sites. This was an increase of over 200 percent since the same period in 2008. BSA requested the removal of over 100,000 torrent files used by nearly 2.9 million people to download software with a retail

* It should be noted that unlike the music and movie industries that estimate actual losses, the BSA figures are for value of the software based on a blended average price. Assuming there is not a one for one substitution rate between pirated and legitimate software copies, actual losses are likely significantly less than the reported value of the pirated software.

value in excess of $974 million. BSA also requested auction site providers to shut down more than 19,000 auctions offering approximately 128,000 products.[143]

Notably, however, business software piracy rates in the majority of countries are stable or declining. In 2009, unlicensed software installations declined in 49 percent of the 111 countries studied by BSA. They remained steady in 34 percent of the countries, increasing in only 17 percent.[144] BSA attributed the declining rates of piracy to anti-piracy programs, including vendor legalization, government education, enforcement actions, and increased use of digital rights management.[145] These declining rates are significant because they demonstrate that anti-piracy efforts may reverse trends.

The shift to digital content is the most significant driver of the accelerating demand for pirated content. First, with digital content it is possible to provide pirated content with no perceivable difference in quality versus legitimately obtained content. Second, the growth of the Internet combined with the expanded availability of broadband has made distribution of pirated content even easier. Digitally pirated music and movies are available using P2P networks, BitTorrent, cyberlockers, streaming sites,[*] or mobile piracy.[**] A study of 43 unique Internet sites responsible for digital piracy determined these sites generated over 146 million visits per day, totaling more than 53 billion visits per year. The top three digital piracy sites together generated over 21 billion visits per year.[146] Third, consumers can obtain much of the content for free using online piracy.[147]

In addition to the pure profit loss to the rights holders, the United States also suffers significant economic losses from piracy. For example, research suggests the United States economy loses over 212,090 jobs, and United States federal, state, and local governments lose a combined $1.279 billion in tax revenue annually from movie and music piracy.[148] Although these estimates are outdated, the magnitude of the losses to the United States economy is still significant.

As noted previously, software piracy may also have a negative impact on national security systems. Some United States government agency computers have already been compromised by pirated software products and foreign governments could use the pirated software to collect intelligence from United States government computer systems.[149] In addition, software pirates use software embedded with malicious code to obtain bank account details, personally identifiable information of employees and clients, and access networks vital to the protection of United States critical infrastructure.[150] For example, an employee of one company downloaded pirated music and video software from LimeWire, a P2P network, onto a work computer. This P2P program allowed outsiders to access the company's computer systems and expose the personal data of about 2,000 clients.[151] Similar downloads by government employees to their work computers could inadvertently expose government networks to unauthorized access.

[*] Streaming websites allow users to listen to or view content on demand without downloading files to their computer.

[**] The streaming and downloading of pirated content to an individual's laptop or mobile phone. With the advent of so-called "smart phones" such as the iPhone and the Android users developed applications ("apps") exclusively for online music piracy. One industry association reported it has identified between 300 and 400 apps that enable music piracy on Android phones.

Business software piracy is also financing organized crime in Mexico. According to Microsoft's lawyers, the sale of pirated Microsoft software funded the Mexican drug cartel La Familia Michoacana's illegal activities, including kidnappings and drug and weapons trafficking.[152]

Pharmaceuticals

Counterfeit pharmaceuticals[*] can be the most serious and pervasive health and safety threat from counterfeit goods. These drugs circumvent all of the standards and protections built into the production and distribution of genuine pharmaceuticals. They may contain too little, too much, or no active primary ingredients and/or various contaminants.[153] Counterfeit pharmaceuticals may cause several types of harm: they may injure or kill someone directly because they contain contaminants such as rat poison, heavy metals, or poisonous chemicals; they may injure or kill directly because they have too much of the active ingredient and cause an overdose; they may injure or kill indirectly because they are missing the active ingredient resulting in people becoming more ill or dying from a treatable condition; and they may kill many in the longer term as drugs with inadequate amounts of active ingredient may lead to more drug resistant diseases.[154]

There are no reliable measurements of the actual quantity of counterfeit pharmaceuticals produced each year. As Randall Lutter, Associate Commissioner for Policy and Planning of the FDA, testified, "The sophistication and precision of some counterfeit copies of legitimate drugs make a reliable estimate of the number of counterfeits impossible."[155] The World Health Organization previously estimated approximately 10 percent of drugs worldwide are counterfeit but the percentage varies widely by country and method of obtaining the drugs.[**156] One research firm estimated the global market for counterfeit pharmaceuticals generate revenues between $75 billion and $200 billion a year.[157] The Pharmaceutical Security Institute (PSI), a pharmaceutical trade association created to address illegal pharmaceutical incidents, collects data on the number of counterfeiting, illegal diversion, and theft incidents. These incidents increased seventy-eight percent from 2005 to 2009.[***] Pfizer reports between 2004 and 2010 it seized more than 62 million doses of counterfeit medicines worldwide.[158] More than 200 million counterfeit Eli Lilly medicines have been seized in 800 raids around the world.[159]

[*] The World Health Organization defines counterfeit pharmaceuticals as medicines that have been deliberately and fraudulently mislabeled as to identity or source in an effort to make them appear to be genuine. The FDA defines counterfeit pharmaceuticals as drugs that are produced, distributed, or sold under a product name without authorization from the rights holder and where the identity of the drug source is knowingly and intentionally mislabeled in a way that suggests it is the authentic and approved product. This definition may encompass pharmaceuticals that are not approved by the FDA but do not violate intellectual property rights; therefore, when this report refers to counterfeit pharmaceuticals it refers to the general definition of counterfeit used across all types of products.

[**] WHO no longer provides such estimates because of the difficulty of providing accurate measurement.

[***] The numbers from 2002 through 2009 show a tenfold increase but, as PSI acknowledges, at least some of these increases are likely due to increased reporting as a result of improved data collection, increased law enforcement efforts, and better public awareness. These numbers also include incidents other than counterfeiting so it is not possible to determine whether counterfeiting incidents rose at a faster or slower rate than diversion and theft incidents. See http://www.psi-inc.org/incidentTrends.cfm.

Counterfeit medicines are not limited to a few countries or illicit venues. A one week worldwide law enforcement effort in 2010, Pangea III, directed at online suppliers of counterfeit drugs identified more than 820 websites engaging in illegal activity, 297 of which were shut down. In addition, law enforcement seized over 11,000 packages of counterfeit drugs and more than 2.3 million illicit and/or counterfeit pills.[160] In 2007, counterfeit pharmaceuticals were seized in at least 45 countries.[161] Pfizer reports counterfeit versions of at least 20 of its products have been found in the legitimate supply chains of at least 44 countries.[162]

The types of drugs being seized have broadened. Counterfeit versions of nearly every type of medicine have been recovered, including those intended to treat heart disease, arthritis, asthma, AIDS, malaria, and cancer.[163] Counterfeit versions of 19 of the world's 25 best-selling drugs have been seized.[164] PSI estimates counterfeit versions of approximately 800 different pharmaceutical products were made in 2009.[165]

Significantly less than one percent of the market value of the drugs in the legitimate supply chain in the United States is believed to be counterfeit.[166] The Internet is the most common source of counterfeit pharmaceuticals purchased by United States consumers.[167] Over 50 percent of the medicines purchased from illegal web sites that conceal their true physical address are believed to be counterfeit.[168] These illegal Internet pharmacies "conceal their real identity, are operated internationally, sell medications without prescriptions, and deliver products with unknown and unpredictable origins or history."[169] These sites are particularly dangerous because consumers generally have no way to determine what is in the medicines they receive.[170] Consumers do not understand the risk of purchasing drugs from these sites. Sixty-three percent of Americans surveyed reported hearing nothing or very little about prescription drugs being made with ingredients that make them unsafe to consume.[171]

Many Americans trust Canadian pharmacies will provide them with genuine drugs identical to what they would obtain from their local pharmacy, only for a cheaper price.[*] In contrast, a poll found 54 percent of Americans distrust drugs made in India and 70 percent distrust drugs made in China.[172] Internet pharmacies fool many customers by implying they are based in Canada. There are fewer than 300 government authorized online pharmacies in Canada but more than 11,000 fake "Canadian" pharmacies operating online from overseas jurisdictions.[173] Some of these "Canadian" pharmacies are based in Russia or India and distribute counterfeit pharmaceuticals produced in China.[174]

Foreign based Internet sites may transship products to evade detection by customs officials and prevent customers from knowing the true source of the drugs. One industry representative described a case where a counterfeit drug manufacturer shipped drugs from China to the Bahamas through Hong Kong, Dubai, and the United Kingdom. The drugs were then placed into small envelopes with patients' names on them. These envelopes were consolidated and shipped back to the United Kingdom. The United States consumers received the drugs through the mail from the United Kingdom.[175]

[*] A survey found 60 percent of Americans had confidence in the safety of prescriptions from Canada. An additional 23 percent were somewhat confident in Canadian prescription drugs. Only nine percent claimed to be not confident that prescription drugs from Canada were safe and free from contamination. See Pew Prescription Project, "Americans' Attitudes on Prescription Drug Safety," April 2010.

With the advent of Internet drug sites, individual dealers of counterfeit drugs can deliver enormous amounts of pharmaceuticals to large numbers of customers. One American convicted of drug counterfeiting reported selling more than $20 million worth of counterfeit drugs through a series of websites. He used the Internet to find finished pills and active primary ingredients in China, India, and elsewhere. He then sold counterfeit versions to 65,000 customers. He explained, "[i]f you are on the Internet, people can't really tell if you are a big operator, a reputable operator, or who you are as long as you can make that website look pretty impressive."[176]

Electronic components

There are no industry-wide estimates of the magnitude of the threat from counterfeit electronic components. Efforts to measure the threat encounter numerous challenges, including that key entities, such as the DOD, do not have a consistent definition of the term "counterfeit" nor a consistent means to identify suspected counterfeit parts.[177] There is no single database in government or industry where all suspected or confirmed counterfeit parts are tracked. In the Commerce assessment, only 2 of the 14 entities that found counterfeits maintained a database of such parts and neither of these organizations was the Defense Logistics Agency, the largest supplier of parts to DOD.[178] The Defense Criminal Investigative Service (DCIS) reports that although it has records of hundreds of non-conforming parts, it does not have codes to distinguish counterfeits from other nonconforming goods.[179]

The Commerce assessment, which focused solely on electronic components, found all elements of the defense and industrial supply chain have been impacted by counterfeit electronic parts.[180] Thirty-nine percent of companies and organizations that participated in the Commerce survey encountered counterfeit electronics between 2005 and 2008.[*181] During that same time period the number of counterfeit electronics incidents detected increased 241 percent, from 3,868 incidents in 2005 to 9,356 incidents in 2008.[**]

Electronic components are the most commonly reported counterfeit DOD parts. In addition to the Commerce assessment results, DCIS and the United States General Services Administration (GSA) reported that almost all of their counterfeit parts cases in recent years involved counterfeit electronics.[182] A March 2010 GAO study reported numerous anecdotal accounts of infringing goods[***] in the DOD supply chain, and approximately two-thirds of reported counterfeiting incidents involved fasteners or electronic parts.[183] Many of the reported incidents involved blacktopping or relabeling of items to make them appear newer or of a higher quality in order to meet government specifications.

---

[*] Surveys were collected from 387 companies and organizations representing the five segments of the DOD supply chain (original component manufacturers, distributors and brokers, circuit board assemblers, prime contractors and subcontractors, and Department of Defense agencies).

[**] The increase may not be due solely to more incidents but may also reflect improved detection efforts and recordkeeping.

[***] GAO noted because definitions of counterfeit vary within DOD, the examples of counterfeit in its study were based on the interviewee's understanding of the term. It noted, however, that generally the examples of counterfeits involved "instances in which individuals or companies knowingly misrepresent the identity or pedigree of a part."

Between November 2007 and May 2010, CBP and ICE seized over 5.6 million counterfeit semiconductor devices. More than 50 of the seized shipments involved counterfeit devices purporting to be military or aerospace grade. The seized semiconductors bore counterfeit trademarks of 87 North American, Asian, and European companies and were destined for 16 countries, including the United States.[184]

A survey of semiconductor manufacturers provides glimpses into the magnitude of the problem. For example, one company estimated two to three percent of purchases of products bearing its brand name are counterfeit. A broker website indicated 40,000 units of a particular device were available for purchase but the manufacturer had only made 200 units with the specified date code. Another company reported 19 cases of counterfeits involving a total of 97,000 units. Another reported having over 100 of its part numbers counterfeited over a three year period.[185]

In 2008, there were large seizures of counterfeit Cisco Systems products, including counterfeit routers, switches, gigabit interface connectors, and WAN interface cards. Purchasers of the counterfeit items included six different United States government entities and a leading defense contractor.[186] In one operation in China over 700 counterfeit Cisco items of network hardware and labels with a value of more than $143 million were seized.[187]

These studies likely underreport the extent of the problem as industry and end users often do not report counterfeit parts. Reasons for not reporting vary but include: time pressure in the field where nonworking parts are discarded instead of reported; personnel working with the parts do not know their source so there is no way to trace them to the original supplier; companies are reimbursed for faulty parts so there is no need to investigate why they are faulty; and concerns regarding legal issues or policies about reporting issues outside one's own organization.[188]

There are no confirmed reports of injuries or deaths in the United States due to counterfeit electronic parts, but this is more likely due to a failure to look for such a cause or destruction of evidence of counterfeit parts in the fire than to an absence of actual harm. Evidence indicates use of counterfeit electronics is widespread, and the potential consequences from counterfeit parts critical to United States infrastructure, such as power plants and dams, as well as defense readiness via United States military systems and other elements of national security, could be immense.

Aircraft parts

There are no industry-wide estimates of the magnitude of the threat from counterfeit aircraft parts. Efforts to measure this threat encounter similar challenges to those encountered when measuring electrical components: there are inconsistent definitions of counterfeit; there is sporadic and incomplete reporting; there is no central repository for data; and there are multiple end uses for the various parts so they are not designated as aircraft parts.

The little available data indicates counterfeit aircraft parts appear in a wide range of types of aircraft, including commercial passenger, military, cargo, and recreational planes.[189] In addition, a diverse range of aircraft parts are counterfeited, ranging from electronics to fasteners to landing gear.[190] Together these facts indicate the seriousness of the problem.

The Federal Aviation Administration (FAA) discontinued its database for tracking counterfeit aircraft parts in 2007.[191] Although FAA once estimated approximately 520,000 counterfeit or unapproved parts are installed on planes annually, it does not segregate figures for counterfeits from the many categories of unapproved parts.[192] The principal database containing reports of counterfeit aircraft parts is the DOD-run Government-Industry Data Exchange Program (GIDEP). It is an information clearinghouse for data related to maintenance, supply, and testing of components used by the United States military and civilian industries. The utility of this database has been limited because of membership restrictions, reluctance to report nonconforming parts because of potential liability issues, and company reporting systems that did not support reporting outside of one's own organization.[193] In addition, repair stations and facilities that are the sources of the reporting may be unable to determine the authenticity of a given part or know how to report parts they suspect are counterfeit.[194]

An analysis of reports between June 2008 and November 2009 of suspected counterfeit parts identified 222 separate incidents where at least one aircraft part was suspected of being counterfeit.[195] Due to the reporting problems described above, this data is not an accurate measure of the extent of the threat. CBP and ICE seizure reports do not offer a perspective as they do not specify whether any aircraft parts were seized in the given year. A review of the underlying 2010 seizure data determined there were no seizures of aircraft specific goods that year. No other statistical measure of the magnitude of the threat in the aircraft industry was found.

The potential impact of counterfeit parts may be considerable. All sources agree counterfeit aircraft parts pose a significant safety concern. Several airplane crashes around the world have been linked to counterfeit parts.[*196] Other aircraft parts failures have been documented but these were redundant components.[197] In addition, counterfeit parts on military aircraft could negatively impact a mission.[**198] One Navy analyst estimates counterfeit aircraft parts are a critical factor in decreasing weapons systems reliability.[199]

Luxury goods and apparel

Counterfeit designer handbags and clothing are classic examples of the large market for counterfeit goods. These goods are sold openly in street markets, flea markets, and online. Shoppers regularly go to places such as Canal Street in New York City and Santee Alley in Los Angeles to purchase known counterfeit handbags, clothes, watches, perfumes, and other brand name goods. These goods are the major component of the secondary market for counterfeit products.

[*] Determining the role of counterfeit parts in any given aircraft accident is difficult because the relevant evidence may have been destroyed in the accident. In addition, accident investigators often are not trained to look for evidence of counterfeits at the scene of the accident.

[**] A counterfeit chip was found in a fighter jet's flight computer. One agency found two counterfeit parts that if installed would have caused mission failure.

While there is no industry-wide measure of the size of the counterfeit luxury goods and apparel market,[***] most indicators demonstrate the problem is large. Among losses to United States interests are industry shares, losses in sales taxes and customs duties, increased expenses in IPR enforcement, and general devaluation of the authentic trademark. While counterfeiting luxury goods and apparel cost rights holders some lost sales, for the true higher end goods such damage is believed to be relatively small because consumers of counterfeit products do not markedly reduce the pool of legitimate buyers.[200] Industry representatives reiterated this idea as they were as concerned with the dilution of their trademark as they were with lost sales.[201] As the quality of counterfeits increases and the ability of Internet sites to convince buyers they are purchasing genuine goods increases, it is expected the impact on sales will increase.

Apparel – which encompasses clothing, accessories (such as handbags), and shoes – is believed to be the single most commonly counterfeited class of goods. Although as a percentage of CBP and ICE seizures these categories have declined in recent years, they still comprise three of the top five categories of goods seized and when combined are the number one category of goods seized. Based on domestic value, footwear alone has been the number one category of goods seized every year since 2006.[202] In 2010, CBP made nearly 10,000 seizures of wearing apparel, footwear, handbags, wallets, backpacks, and watches.[203]

One clothing manufacturer representative estimated 30 percent of global sales of products bearing his company's trademark are counterfeit.[204] A representative of one luxury goods company reported demand and prices for counterfeit versions of his products have remained the same for the past ten years, which he saw as an indication of a consistent supply and demand chain for counterfeit luxury goods.[205]

VI. OFFENDERS

This section focuses on the specific types of offenders who manufacture, produce, and distribute infringing goods – both their motivations for committing these violations and the organization of their operations.

Key Definitions

Criminal enterprise: "a group of individuals with an identified hierarchy, or comparable structure, engaged in significant criminal activity" without the additional elements of violence, corruption, graft, or extortion necessary to be considered organized crime.

Organized crime: "any group having some manner of a formalized structure and whose primary objective is to obtain money through illegal activities" and "maintain[s] their position through the use of actual or threatened violence, corrupt public officials, graft, or extortion." Traditional organizations such as the mafia or triads are common examples.

Members of these criminal organizations have known ties to the organization and participate in the illegal activities of the group.

Sympathizers or ***supporters*** may agree with the ideology of a group and provide financial support to the criminal organization, but do not participate in the primary criminal activities of the organization.

Source: www.fbi.gov/about-us/investigate/organizedcrime/glossary; IPR Threat Report Team.

[***] For the purposes of this report this category includes handbags, shoes, clothing, sunglasses, perfumes, watches and jewelry.

Certain offenders pose a threat not only to the economic interests of rights holders and the United States economy at large, but in isolated cases are also threats to United States national security. The IPR Center distinguishes between the types of criminal organizations (i.e. general criminal enterprises, traditional organized crime, terrorist organizations, and gangs), as well as the different types of participation of offenders in these criminal organizations (i.e. members and supporters). As depicted in Figure 10, there are several types of offenders whose role in IPR violations this report will analyze.

Figure 10: Types of Offenders Responsible for Manufacturing, Production, and Distribution of Infringing Goods Affecting United States Interests

Type of Offender	Subgroups Affecting United States Interests	Primary Motivation	Primary Types of Infringing Goods	Primary Role in IPR Violation	Primary Locations
Individual/Small Groups	United States or foreign non-government sponsored	Profit	Content piracy, counterfeit clothing, trade secrets	Manufacturing, distribution, retail, theft of trade secrets	United States, worldwide
	United States or foreign non-government sponsored	Vengeance	Trade secrets	Theft of trade secrets	United States, China, worldwide
	Foreign non-government sponsored	Theft of sensitive United States information	Pirated software, counterfeit computer hardware	Distribution, theft of trade secrets	United States, worldwide
General Criminal Enterprises (Members)	Asian (Chinese), Middle Eastern	Profit	Content piracy, counterfeit clothing, luxury goods, cigarettes, and pharmaceuticals	Distribution	United States, China, Middle East
Organized Crime (Members)	Asian (Chinese Triads), Los Zetas, La Cosa Nostra, Camorra, Russian Mafia, Japanese Yakusa	Profit	Counterfeit cigarettes, optical discs, software	Distribution	United States, China, Mexico, Italy, Russia, Japan
Terrorist Organizations (Supporters)	Hizballah, D-Company, possibly Al-Qaeda	Profit/Ideology	Content piracy, counterfeit video game devices	Distribution	Tri-Border Area, India/Pakistan, Europe
Gangs in the United States (Members)	Street Gangs (MS-13), Outlaw Motorcycle Gangs	Profit	Counterfeit software, optical discs, clothing	Distribution	United States (California, Southwest)
Foreign Government Offenders	Agents of the Chinese government	Theft of sensitive United States information	Pirated software, counterfeit hardware, trade secrets	Economic espionage	United States, China
Warez Groups	--	Fame	Digital content piracy	"Manufacturing," distribution	United States, worldwide

Source: IPR Center Analysis Team Research

A. Profit Driven Offenders

IPR offenders are motivated primarily by profit. IP theft is attractive to offenders because they produce relatively high profits combined with a perceived low risk of apprehension or significant consequences if apprehended.[*206] Such people operate in a range of organizations, from the relative isolation of a "mom and pop" home operation to large organized criminal networks.

1. Independent and small operators

Although there are IPR cases involving solo or small groups of individuals who operate out of their homes, garages, or small storage facilities,[**207] there is little reporting and no actual analysis of the relative importance of such operators to the threat. Some manufacturing operations, such as optical disc and digital piracy, do not require significant capital, structure, or space in which to conduct these offenses and thus are conducive to small operations. Retailers of infringing goods may be small operators, such as individual stalls in a street market or online sellers at sites such as eBay, Craigslist, or Alibaba. Yet small operators may still cause significant harm. For example, single individuals may steal trade secrets worth hundreds of millions of dollars.[***]

One United Nations sponsored report argues smaller scale counterfeiting "is definitely not close to disappearing."[208] Although this proposition is likely true, the report did not offer any statistical work or other rigorous analysis supporting these conclusions. This lack of reporting and analysis may be a reflection of the fact that individuals and small operations are a less attractive target for law enforcement than larger enterprises engaging in more significant infringing activity or also committing other more serious offenses.

2. Criminal organizations

There are four types of criminal organization offenders: members of general criminal enterprises, members of traditional organized crime groups, supporters of terrorist organizations, and members of gangs. These offenders may use profits from IP theft to fund other illegal activity, or vice versa, use profits from other activities to fund sophisticated, large scale infringing operations.

---

[*] The Administration proposed increasing sentences for IP crimes to alter the risk/reward calculations of potential offenders. See Executive Office of the President of the United States, "Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations," Mar. 2011.

[**] For example, an individual in Massachusetts pled guilty to selling counterfeit clothing and accessories, some of which he manufactured in his basement. See Department of Justice, "Norwood Man Pleads Guilty to Selling Counterfeit Clothing and Accessories," *Press Release*, 23 Feb. 2000.

[***] For example, a single individual pled guilty in November 2010 to stealing trade secrets, valued between $50 million to $100 million from his former employer, Ford Automotive. See United States Attorney's Office Eastern District of Michigan, "Chinese National Pleads Guilty to Stealing Ford Trade Secrets," *Press Release*, 17 Nov. 2010. Similarly, a single individual was charged in 2008 with stealing trade secrets from his employer, Intel. Intel valued the trade secrets he downloaded at $1 billion. See U.S. Department of Justice, "Former Intel Employee Indicted for Stealing more than $1 Billion of Trade Secrets," *Press Release*, 5 Nov. 2008.

Criminal enterprises

Members of general "criminal enterprises" and their subset, "organized crime groups," commit IPR violations. Criminal enterprises in the United States and abroad are profiting from IPR crime.[209] This conclusion is not contentious.[*210] There is, however, little if any evidence demonstrating the relative significance of these enterprises to the threat.

As the nature of infringing operations has evolved, the role of criminal enterprises likely has increased and will continue to do so. The general nature of infringing operations are evolving from smaller operations in a few limited industries that produce obviously fake goods to more sophisticated operations capable of producing high quality and highly technical fakes.[211] Higher quality and more technically sophisticated infringing goods require more capital investment for activities such as reverse engineering, sophisticated manufacturing equipment, and more complicated distribution efforts to penetrate more controlled supply chains. There are many examples in recent years of infringing goods so closely resembling legitimate products that only an expert who dissects the product or conducts scientific tests can determine whether or not the product is genuine.

Members of criminal enterprises commit IP theft in a broad range of industries, including content piracy and counterfeit clothing, luxury goods, pharmaceuticals, and cigarettes.[**] Anecdotal evidence indicates criminal enterprises are predominantly involved in content piracy, counterfeit clothing, and counterfeit cigarettes. These industries have relatively low barriers to entry as little technical expertise is required, the products are easily distributed, there is high demand for these products, and there is relatively little criminal prosecution for these offenses. Because these industries generally do not require a high level of sophistication or technical expertise, they provide a way for criminal enterprises to easily get involved in IPR violations. They can then leverage their organizational strengths to move into more sophisticated, capital intensive operations.

Members of criminal enterprises that affect United States interests are at a minimum involved in the distribution of infringing goods, including importation of goods into the United States. In the case of piracy operations, the criminal enterprises may operate more integrated businesses that extend from the manufacturing of optical discs to distribution of the discs to the end users.[***212]

Criminal enterprises have relatively larger operations than independent and small operators and as a consequence will commit IP theft on a scale that will have a larger negative economic impact as well as generate more profits. Examples include an Asian criminal enterprise of 30 defendants charged with smuggling into the United States counterfeit cigarettes worth approximately $40 million and other counterfeit goods, including pharmaceuticals worth several

---

[*] Indeed, the United States government acknowledged the link between organized crime groups and IPR violations as early as 1996 with the addition of trafficking in counterfeit goods as a predicate offense for RICO (Racketeer Influenced and Corrupt Organizations) charges. 18 United States Code § 1961.

[**] Although it is often reported that organized criminal networks and terrorist organizations are involved with counterfeit cigarettes and counterfeit cigarette tax stamps, it should be noted that counterfeit tax stamps are a fraud offense, not an IPR violation.

[***] For example, members of MA Ke Pei, a Chinese criminal enterprise, who were charged with manufacturing and distributing counterfeit software to the United States.

hundred thousand dollars.[213] The investigation of the MA Ke Pei group resulted in the seizure of counterfeit software in China and the United States worth more than a half billion dollars. [214] Reporting also indicates Middle Eastern criminal enterprises are engaged in multi-million dollar counterfeit trafficking.[215]

Organized crime

Organized crime groups are a specialized subset of criminal enterprises that maintain their position through the use of actual or threatened violence, corrupt public officials, graft, or extortion. For example, members of the Lim Organization, an Asian organized crime group in New York, trafficked in counterfeit goods and were charged with attempted murder and conspiracy to commit murder.[216] Another example is the Yi Ging Organization, a Chinese organized crime group in New York, whose members were indicted for extortion, witness tampering, money laundering, and drug trafficking, in addition to trafficking in counterfeit DVDs and CDs.[217]

Members of organized crime are at a minimum involved in the distribution of infringing goods within the United States. There are many examples of this activity across a variety of organized crime groups. The Yi Ging Organization distributed pirated American and Chinese DVDs and music CDs to stores they controlled across New York City.[*218] Similarly, members of the Lim Organization stored counterfeit goods in warehouses in Manhattan and Queens, New York.[219] According to a United States government representative based in Beijing, Chinese organized crime groups, such as the Big Circle Boys, 14K, and Sun Yee On triads, are involved in the trafficking of counterfeit cigarettes and other counterfeit goods that are delivered to New York City.[220] Dated reporting suggests the Big Circle Boys were previously involved in the distribution of counterfeit computer software, particularly Microsoft software, within the Los Angeles, California area.[221] Foreign government and private industry sources report the Camorra, an Italian organized crime group, distributes infringing goods, such as counterfeit clothing, to the United States. [222] Industry experts report members of Los Zetas, a Mexican organized crime group with a presence in the southwest United States, distribute counterfeit CDs, DVDs, and software. [223]

Asian organized crime groups, such as the Yi Ging and Lim Organizations, are the most common organized crime groups committing IPR offenses in the United States. This conclusion is consistent with the majority of counterfeit goods originating in China. But these offenses are not limited to Asian groups. For example, members of the Gambino organized crime family of La Cosa Nostra (LCN), an Italian mafia in the United States, were indicted in 2005 for the sale of counterfeit luxury goods, including watches and handbags.[224] According to the United Nations, the most notorious organized crime groups involved in IPR violations are the Chinese triads, the Japanese Yakusa, the Italian Camorra, and the Russian Mafia.[**225] The IPR Center found little

[*] In addition to the counterfeiting charges, they were also charged with RICO offenses, including extortion, witness tampering, money laundering, and drug trafficking.

[**] Sicilian Mafia, 'Ndrangheta, Camorra, and Sacra Corona Unita operate in at least 19 states, according to law enforcement reporting. IOC members engage in myriad criminal activities, including assault, counterfeiting, extortion, fraud, money laundering, and drug trafficking. See National Drug Intelligence Center, "Drug Trafficking Organizations," *National Drug Threat Assessment 2009*, December 2008.

reliable information regarding possible IPR violations in the United States by these particular organized crime groups.

Organized crime IPR offenders have specifically targeted law enforcement officers with violence in isolated cases overseas.[*] There also has been isolated reporting regarding organized crime groups using threats of violence to force retailers or individuals to sell infringing products.[226] Such pressure is particularly significant when used to infiltrate legitimate supply chains as it will increase the likelihood consumers will be deceived into purchasing counterfeit goods.

Limited reporting suggests organized crime groups have more extensive resources and networks that allow them to bring more infringing goods to the United States than independent offenders. In addition, these larger networks may create more profits for organized crime groups that could later be used to finance other crimes. One source argued transnational manufacturing and distribution of infringing goods requires "significant amounts of capital and strong organizational links between parties operating across different locations," and organized crime groups are well positioned to provide these resources.[227] For example, the Yi Ging Organization, with at least 39 members in New York as well as business partners or affiliates in China, allegedly earned millions of dollars from its pirated CD and DVD business.[228] The Lim Organization stationed at least 28 members in the United States.[229] In one raid law enforcement officials seized over 322,000 pirated CDs worth over one million dollars from members of Los Zetas, a Mexican organized crime group that distributes counterfeit music CDs and software in Mexico and the southwest United States.[230]

There is little support for claims that criminal enterprises and organized crime groups use profits from IPR violations to fund other criminal activities. Although it is logical to assume members of organized crime groups and criminal enterprises commit IPR violations to earn profits to fund other crimes, no new evidence exists to support such a claim. It is possible that such groups use profits from other crimes to fund IPR violations by investing in sophisticated manufacturing equipment or building networks. It is also possible the profits from IPR violations are simply an income source for these organizations and do not fund other illicit activities.

Terrorist organizations

Terrorist supporters have used intellectual property crime as one method to raise funds. Central to this judgment is the distinction between terrorist supporters who merely provide funding and resources to a terrorist organization versus terrorist organization members who engage in the actual terrorist activities of violence.[**] It is widely reported terrorist supporters may use IPR

[*] For example, a commander of the Economic Investigations Unit of China's Industry and Trade Administration was stabbed and killed by a trader following the commander's seizure of approximately 1,200 crates of this trader's counterfeit liquor. See United Nations Interregional Crime and Justice Research Institute, "Counterfeiting: A Global Spread, a Global Threat." In another example, the Uruguayan Customs Director was shot by four armed gunmen suspected to be tied to the TBA mafia in reprisal for the confiscation of counterfeit merchandise. See Rex Hudson, Library of Congress Federal Research Division, "Terrorist and Organized Crime Groups in the Tri-Border Area (TBA) of South America," 32.

[**] INTERPOL makes this same distinction. According to INTERPOL, the link between terrorist financing and IPR crimes is direct if members of the terrorist group are "implicated in the production, distribution or sale of counterfeit goods and remits a significant proportion of those funds for the activities of the group," and indirect if terrorist

crimes to provide indirect financial support to terrorist organizations, but little current evidence suggests terrorists are engaging directly in IPR crimes to fund their activities.[*] Due to a lack of any rigorous analysis regarding the amount of this funding, no reliable conclusions can be made regarding the magnitude of such a threat to United States interests.

There is some evidence supporting links between IPR violations and Hizballah. A congressional delegation visiting the TBA in South America "learned the Paraguayan authorities had identified at least 50 local individuals involved in raising millions of dollars for Hizballah and other terrorist organizations in the Middle East. These individuals raised funds by a variety of means, including pirating compact discs and selling counterfeit cigarettes, electronic equipment, DVDs, software, and other common household goods."[231] The delegation learned Assad Barakat participated in IPR violations and allegedly transferred millions of dollars to Hizballah.[232] Other open source reporting confirms the link between the Barakat clan, Hizballah, and IPR violations.[233] In addition, Asa Hutchinson, then Under Secretary for Border and Transportation Security, United States Department of Homeland Security, testified in 2003 that Customs Attachés had seen "indications and circumstances that led Customs to suspect that intellectual property crimes and terrorism are linked" in the TBA of South America (Hizballah) and the Philippines.[234]

There have also been isolated instances of Hizballah supporters committing IPR violations in the United States. In 2006, 19 individuals who were Hizballah supporters in Detroit, Michigan were charged with RICO offenses, including trafficking in counterfeit Viagra, counterfeit Zig-Zag papers, and producing counterfeit cigarette stamps.[235] Additionally, in late 2009, law enforcement officials identified a criminal organization in New Jersey and Pennsylvania that committed stolen property and IPR offenses in the United States and was linked to an international group with ties to Hizballah that was procuring weapons, counterfeit money, stolen property, and counterfeit goods.[236]

There are also allegations of possible links between IPR violations and funding for Lashkar-e-Tayyiba (LeT) and, more remotely, a link to al-Qaeda. In 2003, the United States Treasury Department designated Dawood Ibrahim a terrorist supporter for his funding of LeT terrorist activities and his close relationship to al-Qaeda, including allowing al-Qaeda to use his smuggling routes.[**237] The United Nations Security Council lists Ibrahim on its al-Qaeda and Taliban sanctions list.[238] Ibrahim is the leader of D-Company, an international criminal organization operating in India and Pakistan. In addition to its other crimes, D-Company has been involved in film piracy. CBP seized D-Company branded counterfeit discs in early 2005 and law enforcement officials raided six D-Company disc duplicating facilities in Pakistan. The

---

"sympathizers or militants are involved in [intellectual property rights crimes] and remit some of the funds, knowingly, to terrorist groups via third parties." See Ronald K. Noble, "The Links Between Intellectual Property Crime and Terrorist Financing," Text of public testimony, House of Representatives, Committee on International Relations, 16 July 2003 (Noble testimony).

[*] "Most terrorist groups do not take responsibility for the development and control of counterfeit production and distribution; rather they benefit indirectly from funds remitted to them from sympathizers and militants involved in IPC." See Noble testimony.

[**] Ibrahim was named a Specially Designated Global Terrorist by the U.S. Treasury Department. Ibrahim was linked to the 1993 "Black Friday" Mumbai, India bombings, which killed more than 250 people and injured an estimated 713. See IPR Center, "Intellectual Property Crime: Threats to the United States," June 2010, 8.

raids recovered 400,000 pirated discs, hundreds of master copies, and printing plates used to make labels and covers.[239] Due to a lack of transparency into D-Company finances, however, it is impossible to draw a direct link between money D-Company obtained from IPR violations and its support of various terrorist causes. Moreover, the evidence of D-Company's piracy activities is dated. Some have concluded that with the move to online piracy, physical piracy – the mainstay of the D-Company piracy operations – has declined, profits have "plummeted," and smuggling operations such as D-Company's have been replaced by small scale, local production of pirated works.[240]

The IPR Center found one other alleged link between IPR violations and al-Qaeda. In 2002 the media reported Danish Customs seized a shipment of eight tons of counterfeit shampoo and other personal care products shipped from Dubai to Copenhagen. The media also reported the sender of the infringing goods was "a member of al-Qaeda."[241] Ronald Noble, Secretary General of INTERPOL, testified, "we know that al-Qaeda supporters…have been found with [a] commercial size volume of counterfeit goods."[242] However, his prepared statement for the record was more circumspect. In it he stated, "One counterfeiting case has been reported in the media where there are *alleged* connections to al-Qaeda. The investigation into a shipment of fake goods from Dubai to Copenhagen, Denmark, *suggests* that al-Qaeda *may have indirectly* obtained financing through counterfeit goods. . . The sender of the counterfeit goods is *allegedly* a member of al-Qaeda" [emphasis added].[243] No additional evidence was located to support the allegation that the individual responsible for sending these infringing goods was a member of al-Qaeda, or that proceeds from this illegal activity were intended to fund al-Qaeda versus merely for personal gain.[*]

The other commonly cited example of IP theft funding terrorism is an allegation that the 1993 World Trade Center bombing was partially funded by sales from a counterfeit t-shirt ring.[244] Over an eight year period, several sources reported this information with varying degrees of certainty—some stated it as fact[**] while others were more reserved in reporting a possible link between the two activities.[***] Further research traced these claims back to testimony at a 1995 Senate Judiciary Committee at which a private investigator testified merely that "several high-

[*] It is possible Noble had access to classified materials that provided more evidence of such a link but such evidence was never publicly disclosed. Noble testified, however, "It is difficult to know whether the funds from this traffic went directly to al-Qaeda or whether only a part of them were remitted." See Noble testimony. As the goods were seized before being delivered, it is not clear that there were any proceeds to be remitted to al-Qaeda or any other group.

[**] See, e.g., Kathleen Millar, "Financing Terror: Profits from counterfeit goods pay for attacks," *U.S. Customs Today*, Nov. 2002 ("New York's Joint Terroris[m] Task Force reported a counterfeit T-shirt ring had used sales profits to subsidize the bombing of the World Trade Center in 1993."); see also Moisés Naím, *Illicit: How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy*, 2005, Doubleday: New York, 127 ("The perpetrators of the first World Trade Center bombing in 1993 sustained themselves in part from the sale of counterfeit T-shirts from a Broadway storefront.")

[***] See, e.g., John Solomon and Ted Bridis, "Feds Track Counterfeit Goods Sales," *Associated Press Online*, 24 Oct. 2002 ("A counterfeit T-shirt operation in the New York City area was suspected of providing money to various terror groups, including one linked to the bombing.); see also Roslyn Mazer, "From T-Shirts to Terrorism," *The Washington Post*, 30 Sept. 2001, B02 ("According to 1995 testimony before the Senate Judiciary Committee, New York's Joint Terroris[m] Task Force had reason to believe that high-level players who controlled a counterfeit T-shirt ring were using the proceeds to support terrorist groups such as the one that bombed the World Trade Center in 1993.")

level players indicted in a counterfeiting organization were financially tied to terrorist groups such as the one that bombed the World Trade Center."[245] There was no evidence indicating the persons responsible for the World Trade Center bombing directly participated in counterfeiting operations. Except for these media reports, the IPR Center found no evidence the terrorists responsible for the World Trade Center bombing received funds from sales of counterfeit t-shirts.[*] Even if they did, it would be difficult to determine if these specific funds were used to facilitate the 1993 bombing as opposed to personal income.

Regardless of the magnitude of this activity, these reports are of particular concern because of the relative ease of earning high profits from IPR violations and the relatively small amount of money needed to finance a successful large scale attack. It is widely cited the terrorist attacks of September 11, 2001, cost approximately $500,000.[246] IPR crimes easily could raise this amount of money.

Gangs in the United States

Gang involvement[**] in IP theft is of concern because of the elements of fear and intimidation they employ to further their illegal activities and the frequency in which they commit additional serious offenses, such as murder and drug trafficking.[247] According to the National Gang Intelligence Center (NGIC), there are three subtypes of gangs: street gangs, prison gangs, and outlaw motorcycle gangs.[248] Of these three groups, street gangs most often engage in and profit from IP theft, therefore this analysis focuses exclusively on this subtype.

> A ***gang*** is a group or association of three or more persons with a common identifying sign, symbol, or name who individually or collectively engage in criminal activity that creates an atmosphere of fear and intimidation.
>
> **Source**: National Gang Intelligence Center, "National Gang Threat Assessment 2009, January 2009, 3.

Street level gang members most often distribute infringing goods, specifically pirated content and counterfeit clothing.[249] For example, an MS-13 member in the Los Angeles area sold external hard drives loaded with pirated entertainment software.[250] In September 2010, gang members of Florencia 13 and White Fence were arrested selling pirated CDs in Montebello, California.[251] In Texas, an alleged gang member was arrested with several hundred illegally-copied DVDs of currently-playing and recently-released movies and over one hundred illegally copied CDs.[252]

Local gang members also protect infringing goods markets.[253] The incorporation of street gang security and counter-surveillance makes it more difficult for law enforcement officials to apprehend retailers of infringing goods because the security warns retailers of approaching law enforcement. The retailers abandon their goods, preventing their arrest.[254] For example, industry experts report MS-13 controls parts of Santee Alley in Los Angeles, California. Gang

[*] There was evidence that three years after the World Trade Center bombing law enforcement raided a New York storefront with counterfeit t-shirts intended for sale at the Olympics. Media sources alleged the individuals involved with this operation were "followers" of Sheik Omar Abdel Rahman, who was imprisoned for his role in the thwarted effort to bomb several New York landmarks. See, e.g. Moíses Naím, *Illicit,* 127; IACC, "Negative Consequences," 21.

[**] Although gang members in several countries reportedly engage in IP theft, the IPR Center is focusing on gangs located in the United States as these gangs have the most significant negative impact on United States interests.

members offer protection to vendors in the market for a security fee, and several MS-13 members and associates sell pirated CDs, both of which earn profits for the gangs.[255] In Chesterfield, New York, neighborhood gang members patrol the local infringing goods market. Gang members conduct counter-surveillance, warning retailers of approaching law enforcement.[256]

Interviews with industry experts suggest members of street gangs rarely are involved in the manufacturing of infringing goods.[257] In isolated cases gang members manufacture infringing goods, such as a Florencia 13 gang member operating a pirated video game manufacturing lab in his home in La Marida, California.[258]

MS-13 is the most prominent group involved in IPR violations, primarily because of its significant southern California presence. According to industry experts, Long Beach and Los Angeles, California are "hotbeds for piracy" because so many legitimate suppliers of content are located there. Thus, IPR violators have easier access to original content to pirate.[259] Other gangs located in these areas linked to involvement in IP theft are the Crips, Florencia 13,[260] and White Fence.[261]

B. Offenders Stealing Sensitive United States Information

Other violators commit IPR offenses to undermine the national security of the United States by acquiring sensitive information with United States national security implications, such as weapons designs or defense technology. These offenders may use infringing goods, such as computer software or hardware, with built in spyware or other malware to steal trade secrets or obtain sensitive United States intelligence.[262] They may also use counterfeit integrated circuits which also raise national security concerns "because the history of the device is unknown, including who has handled it and what has been done to it. The devices can also be altered and certain devices can be preprogrammed. Counterfeits can contain malicious code or hidden 'back doors' enabling systems disablement, communications interception, and computer network intrusions."[263] Foreign governments may direct these individuals to steal United States intellectual property.[*] These offenders pose a potentially grave national security risk, including threatening United States war fighters from potentially malfunctioning equipment.

Pirated software poses a likely computer network exploitation (CNE)[**] threat to United States government networks, critical infrastructure, and private networks and systems. Pirated software and/or counterfeit computer hardware could allow access to systems to gather sensitive or proprietary information, conduct cyber attacks, or obtain personally identifiable information to commit identity theft or financial fraud.[264]

[*] China – as a major source of the world's pirated software and the primary source of known assaults on United States government computer systems – is generally considered the most likely to use this method to compromise United States systems for intelligence-gathering purposes. See e.g., Brian Grow, Keith Epstein, Chi-Chu Tschang, "The New E-spionage Threat," *Businessweek*, 10 Apr. 2008, www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm.

[**] A Computer Network Exploitation (CNE) enables operations and intelligence collection capabilities conducted through computer networks to gather data from target or adversary automated information systems or networks.

There has not been a systematic analysis to determine the number of cases in which offenders specifically targeted United States government systems using infringing goods to obtain sensitive information.[*] Although evidence indicates hackers often try to access sensitive government systems,[**] these hackers use intrusion tactics as their methodology, not IPR violations. As such, the magnitude of this threat cannot be measured with confidence.

Offenders intentionally use pirated software to obtain sensitive personal information from United States companies. As a result, software piracy threatens the security of United States business computer networks. Pirated software with hidden malicious code has allowed offenders to obtain bank account credentials, personally identifiable information of employees and clients, and access networks vital to the protection of United States critical infrastructure. Employees installed the majority of the pirated software on the affected computers by visiting pirated software sites or installing P2P software on the computer, suggesting pirates are opportunistic and target employees who engage in these risky computer behaviors.[265] For example, an employee of one business downloaded and installed a pirated version of Adobe Acrobat onto the company's network. The intruder remotely accessed the network through the backdoor created by the software, and attempted to transfer more than $100,000 from company accounts.[266] Another hacker compromised a Pennsylvania water filtering plant's computer system and attempted to covertly use the system to distribute pirated software. The hacker planted malware on the system capable of affecting the operations of an important piece of United States critical infrastructure.[267]

Foreign governments could use pirated software to collect intelligence from United States government computer systems. As noted earlier, a pirated copy of software containing a Trojan virus was installed on an unclassified computer. These viruses are capable of allowing attackers to exploit access to the computer networks through the infected computer.[268]

Although the gravest threats are to sensitive United States government systems with national security information or that control critical infrastructure, other attacks targeted United States businesses using malware included in pirated software. Although in isolated cases offenders targeted certain systems, it is possible other systems were simply targets of opportunity because pirated software made them vulnerable.

For example, several local and state government offices, including a police department, fire department, 911 dispatch, and schools in one state, purchased computer systems that contained pre-loaded, pirated versions of Microsoft Office. The pirated software prevented users from receiving updates needed to protect the computers from cyber attacks and left the computers extremely vulnerable to computer intrusions.[269] In another example, a review of the information

[*] "[I]ncidents of malicious cyber activity targeting the U.S. government cannot easily be quantified due to classification restrictions and fragmentary reporting." See U.S.-China Business Economic and Security Review Commission, "2010 Report to Congress," Nov. 2010.

[**] According to a 2007 Congressional Research Service Report, over 12 million attempts to hack into U.S. government and industry systems were reported in the first six months of 2005. DOD officials indicate the majority of cyber attacks against DOD and U.S. civilian agency systems are suspected to originate in China, and these attacks are more numerous and sophisticated than attacks from other malicious offenders. See Clay Wilson, CRS Report for Congress, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," 15 Nov. 2007.

technology infrastructure in a township in another state revealed most of the Microsoft products on its network were pirated.[*270]

C. Fame-motivated Offenders: Warez Groups

A third, but significantly less common motivation for committing IPR violations is personal fame and notoriety. These individuals are often members of "warez groups," sophisticated and hierarchical criminal groups operating in the United States and abroad that specialize in distributing infringing movies, music, and software via the Internet. Warez group members have varying responsibilities, including supplying, cracking, and ripping the content. Members may include computer savvy who crack access and/or copy codes to distribute content "because they can," or simply to show off their hacking skills.[271] Members sometimes obtain content from industry insiders. For example, a member may obtain a copy of a pre-released film from an industry insider and make the content publicly available via the Internet.[272] Experts from both the film and music industries explained members of alleged warez groups will post multimedia content on the Internet for free to gain notoriety for their computer skills and/or because they believe everyone should have access to music and movies for free. Music and movies obtained from warez groups often make their way to streaming or file sharing sites to allow people to take advantage of free music and movies.[273] For example, one warez group recorded movies at pre-release screenings and posted the films online.[274] Other warez groups obtained physical copies of a film, eliminated the disc's copyright protection or encryption, and posted its content on the Internet free of charge. Warez groups can pose a threat to United States intellectual property from anywhere in the world.

D. Vengeance Motivated Offenders

A final small subset of offenders commits IPR violations motivated by vengeance against the owner of specific intellectual property. Although vengeance motivated offenders could engage in numerous forms of IPR violations, these individuals most often are disgruntled employees who steal trade secrets from their employers. While these particular crimes are not motivated primarily by profit, the rights holder can suffer significant economic losses.[275] These offenders typically steal trade secrets after their employer commits a perceived injustice against them, such as firing or demoting the employee. For example, one individual was charged with stealing trade secrets from ENK International LLC, a trade show organization based in Manhattan that serves the fashion industry, after the company fired her.[276] All industries with trade secrets have the potential for fired or disgruntled employees to steal trade secrets for revenge against a company.

VII. SOURCE OF THE THREAT

Individuals and organizations in foreign countries are the principal source of the threat to United States IP interests. These foreign actors often operate without fear of enforcement in their own

[*] Although the vendors who installed pirated versions of the Microsoft products may have done so solely as a marketing tool to get an edge over their competitors, the existence of pirated software on these computer systems increased the vulnerability of these state and local Government computer networks to cyber intrusions.

countries. The United States Trade Representative's 2011 Special 301 Report places 12 countries on its priority watch list and another 28 on its watch list.[277] There is overwhelming evidence production of counterfeit goods is conducted principally outside the United States and these items cross an array of borders to get to purchasers of the products. The one exception is domestic consumption of pirated works produced within the United States.

The external threat has expanded greatly with the globalization of industry and the declining relevance of borders. Companies may produce legitimate goods in multiple countries and even different levels of production may occur across borders, making the origin of goods less clear. Free trade agreements ease the movement of goods across borders so they may move from suspect countries to countries with which the United States has less concern. The growing influence of the Internet eliminates the high barriers that borders used to pose as producers can inexpensively reach potential customers anywhere in the world and conversely customers can search for sellers anywhere in the world without leaving home.

To examine the extent of the external threat to United States rights holders the IPR Center examined the threat posed by offenders in four countries: China, India, Russia, and Brazil (with special emphasis on the TBA with Argentina and Paraguay). These countries were chosen because of their special significance to the overall threat picture. The IPR Center also examined the internal threat posed by infringement activities occurring within the United States. The IPR Center found the level and type of threat to the United States' interests varies from country to country. As is seen in Figure 11, offenders in China pose the greatest threat in terms of types of infringement and the number of different types of threat. As will be discussed below, it dwarfs the other countries in terms of quantity of infringing goods sent to the United States. Next are offenders in India, primarily because of the increasing role of offenders producing counterfeit pharmaceuticals sent to consumers in the United States through Internet purchases. Offenders in the United States are most responsible for theft of trade secrets, domestic distribution of infringing goods, and production of pirated content. Offenders in the TBA potentially use content piracy profits to fund terrorist groups. The biggest threat to United States interests from offenders in Russia is the extensive content piracy but this is generally limited to internal consumers.

Figure 11: Potential Threats to United States Interests from IPR Violations, by Country of Origin

Country of Origin	IPR Infringement of United States Rights Holders	Potential Threats to United States Interests		
		Economic Interests	Health and Safety	National Security
China	Content Piracy	X		X
	Theft of Trade Secrets/Economic Espionage	X		X
	Counterfeit Luxury Goods and Apparel	X		
	Counterfeit Pharmaceuticals	X	X	
	Counterfeit Electronics	X	X	X
	Counterfeit Automobile Parts	X	X	
	Counterfeit Aircraft Parts	X	X	X
India	Counterfeit Pharmaceuticals	X	X	
	Counterfeit Automobile Parts	X	X	
	Content Piracy	X		X
United States	Distribution of Counterfeit Parts	X	X	X
	Theft of Trade Secrets	X		X
	Content Piracy	X		X
Brazil (TBA)	Content Piracy	X		X
	Counterfeit Aircraft Parts	X	X	
Russia	Content Piracy	X		

Source: IPR Threat Report Team

A. China

China-based IPR infringement is the dominant source of the threat to United States IP interests. Although the magnitude of the threat posed by China-based IPR violations cannot be measured precisely, offenders in no other country approach the level of threat posed by offenders in China. China-based offenders participate in all aspects of illicit production, exchange, distribution, and consumption of counterfeit goods, pirated content, and theft of trade secrets. As a result, China continues to be on the United States Trade Representative's 2011 Priority Watch List.[278]

A: Fujian
B: Guangzhou and Shenzhen, Guangdong Province
C: Shanghai
D: Sichuan

Source: CIA World Factbook

1. Background

China's role in the world economy has grown significantly over the past two decades. In 2010, China's Gross Domestic Product (GDP, on a purchasing power parity basis) was $9.872 trillion, second only to the United States.[279] China's population of 1.3 billion, an estimated 300 to 500 million of whom are middle class,[*] is the largest potential market for goods and services in the world.[280]

China's increasing role as the manufacturing center for the world has fueled its economic growth.[281] With the availability of inexpensive labor and low costs to build and operate manufacturing facilities, China is the site of significant legitimate manufacturing. Domestic and foreign companies produce a vast array of goods in China that are then sold around the world. As a result, China became the world's largest exporter in 2010.[282] Twenty percent of China's exports come to the United States. China is the largest source of imports to the Unites States.[283] At the same time China has developed an informal economy in goods that infringe IPR of both

[*] China's middle class is as large as or larger than the entire population of the United States.

foreign and domestic entities. As noted earlier, the majority of the infringing goods seized each year by CBP and ICE originated in China.

Foreign technology currently fuels 60 percent of the Chinese economy. The Chinese government's economic strategy seeks to reduce the role of foreign technology to 30 percent and decrease China's role of assembling other countries' technology.[284] The Chinese government has a comprehensive coordinated strategy for science and technology development that began in March 1986 with its "863" program.[*285] Chinese government policies "encourage growth and investment in key industries, among which are software and integrated circuit industries. Such policies include foreign investment incentives, tax incentives, government subsidies, technology standards, industrial regulations, and incentives for talented Chinese students studying and working overseas to return to China."[286]

The Chinese have pursued foreign direct investment, particularly from the United States, to transfer production, technology, and research and development to China in return for access to the Chinese market.[287] As a result of these policies, major high-technology companies have built research installations in China. By mid-2004 the Chinese government had registered over 600 such facilities, many belonging to large United States based multinational corporations.[288]

The Chinese government furthered its pursuit of technological and scientific IP leadership with the issuance of its 2006 Medium- to Long-Term Plan for the Development of Science and Technology. This plan institutionalized the concept of "indigenous innovation," a program that by its terms requires the transfer of foreign technology and IP from the original rights holders to Chinese entities in exchange for access to major aspects of the Chinese market.[289] Although China views this plan as necessary to reducing its dependence on foreign technology for critical sectors, the United States Chamber of Commerce reports its companies have called the indigenous innovation plan "a blueprint for technology theft on a scale the world has never seen before."[290] To date, enforcement of the indigenous innovation policies has not occurred; therefore its actual impact is yet to be seen.[**291]

2. The nature of the threat

Offenders in China pose an evolving, large scale threat to the United States IP interests. The USTR noted that although the China-based IPR threat was originally "a localized industry concentrated on copying high-end designer goods" it has become "a sophisticated global business involving the mass production and sale of a vast array of fake goods."[292] Investigations into IPR violations demonstrate China-based counterfeiters are developing increasingly sophisticated techniques for copying legitimate products, counterfeiting a broader range of more and more technical products, and developing new distribution methods to minimize the risk of interdiction. China-based companies produce counterfeits of every type of product and use every technique discussed in Section IV of this report.

---

[*] The 863 program is China's government funded technology development program intended to develop indigenous technological advances and decrease China's dependence on foreign technologies. Its name reflects its inception in March 1986.

[**] At meetings of the U.S.-China Joint Commission on Commerce and Trade on December 2010 the Chinese agreed to several actions that would affect the implementation of the indigenous innovation initiative.

The primary area of production of counterfeit consumer goods in China is in the south of the country, near Guangzhou in the Guangdong Province.[293] One rights holder estimated manufacturers in Guangdong Province produce 70 percent of all counterfeit consumer goods worldwide.[294] Certain types of goods tend to be produced in particular areas of China. For example, manufacturers in the Sichuan Province concentrate more on producing counterfeit technology products while manufacturers in the Hunan and Sichuan provinces concentrate on producing counterfeit pharmaceuticals.[295]

Improved quality counterfeits

Counterfeiters in China have improved the quality and increased the variety of counterfeit goods they produce. They may produce an assortment of different grades of counterfeits to meet demand in different segments of the counterfeit market. For example, retailers at the Beijing Silk Market showed the TDY China Team different grades of counterfeit Louis Vuitton bags. "A" grade bags are a very high quality imitation compared to "B" or "C" grade copies.[296]

In other cases, such as blacktopping of electrical components, the trademarks appear genuine, making it difficult for legitimate companies to determine if a product is theirs without x-raying the part to see the interior. Counterfeiters in China possess the laser equipment necessary to mark electrical components with trademarks identical to the genuine product.[297] Rights holders described the process Chinese counterfeiters often use to create a high quality counterfeit chip. First, they melt the lead solder to retrieve the old chip from a recycled computer circuit board. Then, they clean up the chip, remark it (suggesting it is new), and sell it online.[298] Consumers in the United States often purchase these chips.[299]

The counterfeiters are paying more attention to details that will deceive buyers into thinking they are purchasing the genuine product. For example, seizures of software packages in China contained counterfeit holograms, registration materials, and other critical details that made discerning whether the goods were authentic or pirated difficult for non-experts.[300] By thoroughly mimicking the genuine item, the counterfeiters are no longer aiming for the lower price secondary market. If buyers believe they are buying genuine goods, they will be willing to pay a higher price, which in turn improves the counterfeiter's profits.[301]

Industrial espionage

China's push for domestic innovation in science and technology appears to fuel greater appropriation of other countries' science and technology IP. Offenders in China reverse engineer products, label them as genuine, and sell them in the primary market.[302] There is growing evidence that China desires a faster means to access foreign technology. The U.S. - China Economic and Security Review Commission (China Commission) cautions China's approach to faster development of sophisticated technology includes "aggressive use of industrial espionage."[303] One commentator alleged IP theft and infringement of IPR is part of Chinese companies' business model.[304] Chinese manufacturers are stressing their ability to deliver products identical to those of United States and European companies at prices 15-20 percent

lower. Some observers suspect Chinese companies are using Western patent filings "like recipe books."[305]

China-based espionage efforts have helped the country attain technological developments in two or three years that would normally take ten.[306] David Szady, the former chief of FBI counterintelligence operations, alleges Chinese industrial espionage focuses on systems, designs, and materials. He also argued China is "going after both the private sector, the industrial complexes, as well as the colleges and universities in collecting scientific developments that they need."[307] The China Commission concluded China is using its large network of overseas researchers and students to acquire confidential scientific and technological information from foreign companies.[308] The Intelligence Science Board found "the globalization and growth of multinational corporations and organizations is blurring the distinction between government and commerce, making it difficult to distinguish between foreign-based corporate spying and state-sponsored espionage."[309]

Six of the seven economic espionage cases indicted since the passage of the economic espionage law in 1996 involved the Chinese government.[*] If law enforcement cannot link industrial espionage matters to a foreign government, the United States will charge the offenders with theft of trade secrets. Based on an analysis of trade secret investigations from 2004 to 2008, offenders with links to China represent the most serious foreign threat to United States trade secrets. Although the number of theft of trade secrets cases with a known foreign nexus is limited, over half of those with a foreign nexus have a known link to China. Several cases involved the automobile industry. The remaining cases with known links to China covered a broad range of industries.[310]

In China, it is common for employees of legitimate businesses to leave and create their own companies to make counterfeit copies of their former employer's goods.[311] Although many theft of trade secrets cases involve current or former employees of the victim companies, having an insider is not essential for effective theft of trade secrets. Computer intrusions from abroad have successfully penetrated United States government and defense contractor systems. For example, in June 2007 "the Office of the Secretary of Defense took its information systems offline for more than a week to defend against a serious infiltration that investigators attributed to China."[312] In 2007 and 2008 attacks on a defense contractor system successfully exfiltrated "several terabytes of data related to the design and electronics systems" of one of the United States' "most advanced fighter planes." These attacks were also believed to have originated in China.[313]

The late 2009 attack on Google Inc., an intrusion which included an estimated additional 33 or more victim companies, also resulted in the theft of IP.[314] During the investigation of this intrusion, investigators determined the attack appeared to originate from within China.[315] Google Inc. shut down parts of its China-based business operations because the intrusion posed such a serious threat to the company.[316] Though not specifically commenting on this attack, the China Commission noted the extensive role of the Chinese government in computer exploitation

[*] The other case involved Japan. This information was confirmed by the FBI's Counterintelligence Division, Counterespionage Section.

schemes and stated the government's role "varies from direct participation to some degree of sponsorship or simply acquiescence."[317]

Many of the offenders in China-linked theft of trade secrets cases are Chinese-born, naturalized United States citizens or possess various visas to work or study in the United States.[318] The perpetrators who are not ethnic Chinese develop a relationship with a business in China.[319] Many of the defendants in these cases are engineering, science, or research professionals contributing to development of new products or technology.[320] Many of the offenders were current or former employees of the businesses they victimized.[321] Most of these individuals had direct access to the information stolen because they required the information to perform their duties or had access to databases where it was stored.[322]

Many of these cases involved physical removal of the protected information. Physical removal primarily is conducted through unauthorized copying of files to a portable storage device but some offenders kept laptop computers from a prior employer that contained proprietary information.[323] In other situations the offender, while still employed at the company, gained access to an employer's databases to copy files.[324] One case involved a former employee installing a backdoor to a server to allow him to access and transfer information from his former employer's computer systems.[325] This latter approach has the potential for unfettered data exfiltration and could be a serious threat to the national security of the United States if the information involved is sensitive or export-controlled data.

One rights holder reported his company manufactures its products in phases at different facilities so there are several intermediate stages before the final product is completed at an assembly plant. This elaborate process ensures the company's IP is not concentrated in one location for employees or others to steal.[326] Although this might protect against an insider who only sees one part of the process, sophisticated electronic spying may make such precautions ineffective.

Thwarting customs officials

CBP and ICE seizures of infringing goods from China increased 278 percent from 2005 to 2006. Seizure levels have remained high since that time. Significant evidence indicates counterfeiters are adjusting their shipping methods in order to circumvent law enforcement efforts. Most goods shipped to the United States from China arrive by sea in shipping containers.[327] Based on a belief that shipping containers from China will receive more scrutiny because of the higher likelihood they will contain counterfeit goods, counterfeiters are using several different techniques to avoid such scrutiny.

First, offenders in China are transshipping goods through other countries to disguise the country of origin (i.e. China).[*] The goods may be unloaded in another port and then reshipped in an attempt to sever the link between the goods and China. Second, they use shippers with clean records to decrease scrutiny of their shipments. Third, they will hide counterfeit goods with genuine goods to decrease detection. Fourth, when possible, the counterfeiters send smaller shipments via the postal service or delivery companies, such as FedEx and DHL, which are less

[*] Although they are required to indicate the country of origin regardless of where the goods have traveled there is no evidence that counterfeits are not willing to "counterfeit" the country of origin as well as the goods.

likely to attract attention. If these shipments are seized, they represent a smaller loss than an entire container.[328] One counterfeiter stated he now sends items by United Parcel Service (UPS) because 80 percent of his counterfeit goods successfully get past United States Customs.[329]

A fifth method is to send unbranded goods that customs cannot seize, as they do not infringe on another's trademark. Infringing labels are either shipped separately in a smaller package to the same destination or produced in the destination country and then affixed to the goods.[330] In a sixth model, with the increase in Internet sales, distributors drop ship individual orders from China to the end buyer to decrease the chance United States Customs officials will interdict any particular package.[331]

3. The magnitude of the threat

The OECD assessed China is one of the top source countries of counterfeit goods in international trade.[332] The World Customs Organization notes two thirds of counterfeits detected worldwide come from China.[333] Although it did not provide any quantification of the threat from China-based IP theft, the USTR concluded there is "widespread IPR infringement" affecting "products, brands and technologies from a wide range of industries, including movies, music, publishing, entertainment software, apparel, athletic footwear, textile fabrics and floor coverings, consumer goods, chemicals, electrical equipment, and information technology among many others."[334]

Many rights holders estimate virtually all of the infringement of their products originates in China. One industry representative explained counterfeiters in China produce 99 percent of the counterfeits of his company's products.[335] Another company representative believes 100 percent of counterfeit versions of his company's products come from Shenzhen, China.[336] One luxury brand owner estimated 95 percent of all United States Customs seizures of counterfeits of that brand's goods from 2004 through 2010 originated in China.[337] One footwear manufacturer believes ninety percent of the company's goods were exported from China.[338] A sportswear company executive estimated 97 percent of the counterfeits of his products come from China.[339] Every rights holder the analytic team interviewed listed China as the largest threat to its IPR. China's reputation is as the counterfeit "workshop of the world."[340]

Figure 12:

China's Share of CBP Annual Seizures

Fiscal Year	Number of Seizures	Percentage of Seizures	Percentage of Domestic Value
2010	14,301	61	66
2009	10,288	69	79
2008	10,325	69	81
2007	9,685	71	80
2006	10,325	70	81

Source: U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, "Intellectual Property Rights Seizure Statistics," Fiscal Years 2006-2010.

United States CBP and ICE seizure statistics consistently indicate China is the source country for the majority of goods seized. In 2010, 66 percent of the domestic value of CBP and ICE's seizures involved goods that originated in China.[*341] The next largest source was Hong Kong,

[*] China is also the source of the majority of goods seized by European Customs, accounting for 64.4 percent of goods seized in 2009.

with 14 percent of the domestic value, and Turkey was third with five percent. CBP and ICE's statistics indicate the seizures of goods originating in China were on average of higher value than goods seized originating from other countries.* Fifty-six percent of the value of the seized goods from China were apparel items, including shoes, clothing, and accessories such as handbags, wallets, jewelry, and eyewear.[342] Although China's overall share of the number of seizures declined in 2010, the actual number of seizures increased.**

Of the counterfeit goods posing a health and safety risk seized by CBP and ICE in 2009, 62 percent were shipped to the United States from China.[343] Offenders in China, along with India, produce the overwhelming majority of the counterfeit drugs manufactured worldwide each year.[344] Based on domestic value, 60 percent of the counterfeit pharmaceuticals CBP and ICE seized in 2009 originated from China. This percentage may be larger because some pharmaceuticals are shipped to India, where intermediaries may label or repackage the products before shipping them to consumers in the United States.[345] Other types of dangerous counterfeit products include perfumes, toothpaste, and other personal goods containing hazardous chemicals, electrical components that may catch fire, counterfeit computer components for critical missions, and counterfeit tourniquets.

The demand for counterfeit goods made in China is not limited to exports from China. One study estimates 15 to 20 percent of the goods sold in China are counterfeit and 8 percent of China's Gross Domestic Product (GDP) is comprised of counterfeit goods.[346] With a large and increasing Chinese middle class, there is a large internal demand for infringing goods supplied by Chinese counterfeiters. Thus, United States rights holders are losing sales in the largest market in the world.

Retailers openly sell infringing luxury goods in markets across China. The USTR has repeatedly included Beijing's "Silk Market" on its list of "notorious markets" due to "severe IPR violations."***[347] The TDY China Team visited the Silk Market ("Xiushui Street Market") and observed innumerable infringing goods. When they inquired about purchasing a Louis Vuitton handbag, a retailer showed them a book with pictures of available bags. When they selected bags to consider, the retailer called someone in another location, who then brought the requested bags to the TDY team. The retailer demonstrated the differences between the bags he openly acknowledged were counterfeit. He explained the difference between high quality "grade A" bags versus lower quality "grade B" and even "grade C" bags. On another floor, trays of high quality counterfeit Rolex and other brand name watches were visible. There was booth after booth of vendors selling counterfeit apparel.[348] Chinese government sponsored tourist maps in Beijing direct shoppers to another similar market where the map proclaims shoppers can purchase counterfeit luxury goods.[349] Shenzhen, just across the border from Hong Kong, is well known for offering an array of counterfeit goods from which to select.

* This may be due to higher value goods being seized or more of seizures were of containers of goods versus smaller mail shipments.

** If seizures from China and Hong Kong are combined, their combined relative share of CBP seizures increases slightly in 2010 moving from 79 to 81 percent of seizures.

*** The USTR has also included the Luowu Market in Shenzhen and the China Small Commodities Market in Yiwu on its list of "notorious markets."

The music, movie, and software industries reported "severe losses" due to piracy in China.[350] In a survey of its members, the U.S.-China Business Council identified IPR piracy as the top issue in China for the United States' software, music, and film industries and is fundamental to their business.[351] IIPA estimated 90 percent of the music and movie copies in China are pirated.[352] It further estimated losses from physical music piracy in 2009 in China were $466.3 million.[353] There is a thriving trade in counterfeit optical discs, which most often are sold in small retail shops.[354] The RIAA estimates plants in China have the capacity to produce 4.8 billion CDs a year.[355]

According to the IIPA, in 2009 United States software publishers suffered nearly $3.1 billion in trade losses from piracy in China.[*356] BSA estimates approximately 79 percent of the business software used in China is pirated.[357] There does appear to be some improvement regarding pirated software, as new rules require computers be sold with the operating system software already installed and the government is instituting a new program to ensure government computers only use licensed software.[358]

China also has health and safety concerns from counterfeit products. One United States government official in Beijing estimated 30 percent of the pharmaceuticals in China are counterfeit compared to 1 percent in the United States.[359] In 2004, 13 Chinese babies died and hundreds were malnourished after ingesting counterfeit baby formula with no nutritional value.[360] Yamaha estimates five out of six motorcycles bearing the Yamaha trademark in China are counterfeit. The purchasers of the counterfeit bikes are not only getting one or two counterfeit parts but rather an entire vehicle consisting of parts not authorized or assembled and tested by the legitimate manufacturer.[361]

4. Offenders

The array of offenders operating in China ranges from the small entrepreneur running village-based operations, to large criminal enterprises managing sophisticated fully-integrated operations, to direct support of the Chinese government in economic espionage cases. The roles of these various offenders were discussed in Section VI.

5. Enforcement environment

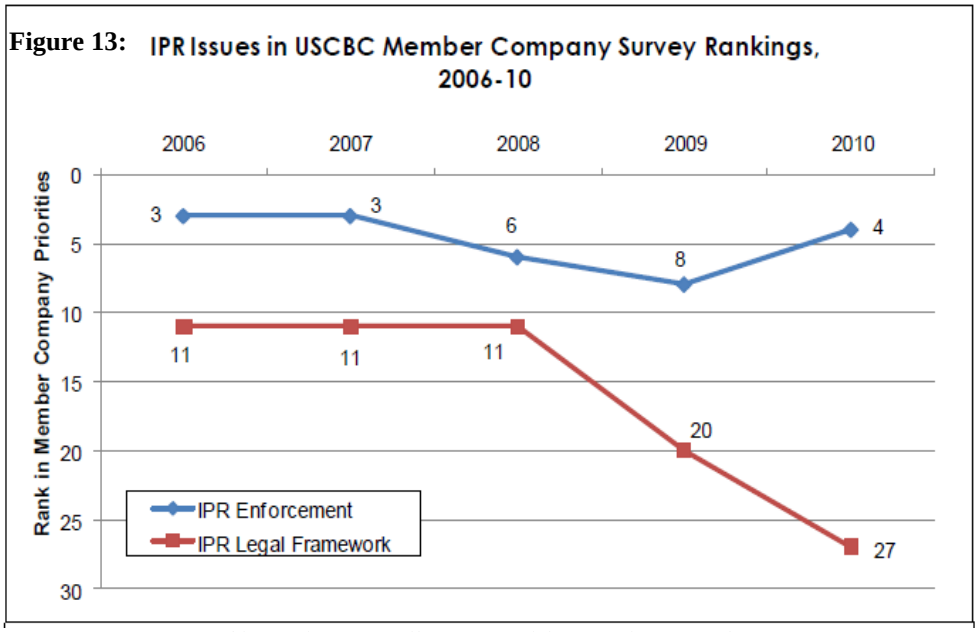
Evaluators of the China IPR environment uniformly conclude the statutory framework in China is adequate for effective enforcement of IPR.[362] As a condition for joining the WTO in 2001, China was required to demonstrate its compliance with the TRIPS Agreement's (Trade-Related Aspects of Intellectual Property Rights) minimum requirements. Despite having adequate laws, the USTR has concluded China's IPR enforcement "remains largely ineffective and non-deterrent."[**363] The results of the recent U.S.-China Business Council member survey provide

[*] Although IIPA does not report equivalent losses in the United States from such piracy, its loss figures are based on BSA data regarding the value of unlicensed software in a country. According to the BSA data, the commercial value of the unlicensed software in China is second only to the value of such software in the United States.

[**] Although in its most recent review the USTR has noted some improvements in China's IPR enforcement efforts, the USTR noted concerns that such efforts would not continue beyond the period of China's designated "special campaign." See USTR, "2011 Special 301 Report," 19-20.

further evidence of the dichotomy between the legal framework and actual enforcement of IPR violations. Since 2008, concerns regarding China's IPR legal framework have declined significantly. Concerns regarding actual enforcement have recently trended upward.

Figure 13: IPR Issues in USCBC Member Company Survey Rankings, 2006-10



Source: The U.S.-China Business Council, "2011 Special 301 Review," 15 Feb. 2011.

Chinese officials can and have enforced IPR laws when there are direct China interests at stake.[364] The most common example is China's aggressive enforcement against IP theft involving the trademarked logos and other symbols associated with the 2008 Summer Olympics.[365] Similarly, a recent Internet enforcement campaign resulted in 558 cases investigated and 375 websites shut down.[366]

Despite this evidence of progress, many obstacles remain. First, although the central government is responsible for passing laws and enacting policies governing protection of IPR, enforcement remains the responsibility of local authorities.[367] An academic the IPR Center interviewed noted, however, the central government has little actual control over the actions of the provincial and local authorities, making enforcement inconsistent.[368] Shanghai, a sophisticated business environment, and nearby Zhejiang are noted for more robust enforcement efforts and local judges knowledgeable in IP issues. In contrast, the USTR and others consider enforcement in provinces in the south of China, such as Guangzhou, where much of the illegitimate manufacturing occurs, significantly less effective.[369]

Due to the lack of adequate law enforcement personnel training, local protectionism, and corruption, IPR enforcement is less likely to occur in areas further from larger cities.[370] For example, if the local authority is related to the owner of an infringing factory, enforcement is less likely.[371] Similarly, if an investigation leads to a state-sponsored entity, IPR enforcement is considered unlikely.[372] Local officials have little incentive to enforce IPR of foreign based entities aggressively because local factories producing counterfeit goods are critical to employment and the economic base of some cities.[373] As one foreign rights holder stated, in

such a case, "enforcement is not an option."[374] These factors make IPR enforcement in China "highly uneven across cities and provinces."[375]

Second, China's policies create a significant incentive for content piracy. The government requires foreign content providers to obtain approval from government censors prior to legitimately distributing the content within China. There is no legal protection for content in China until the censors approve its distribution. Thus, rights holders have no recourse against pirates who distribute unapproved content. By the time the rights holder obtains approval, distributors have saturated the market with pirated content and weakened the legitimate market.[376]

The United States government submitted an official complaint to the WTO regarding China's treatment of IP theft. The first concern was the high minimum thresholds for criminal prosecutions of IPR violations. These minimums are high enough to act as a loophole for smaller producers and violators.[*377] The second concern was the failure to provide copyright protection to content while it was awaiting review and approval by government censors. The third concern was China allowed seized goods to reenter the market as opposed to destroying the goods after removing the infringing label. In January 2009, the WTO ruled China was not complying with its WTO obligations by not protecting content under review and mishandling the disposal of seized goods. The WTO indicated it needed more information on the threshold issue, but China did lower the minimum copyright threshold from 1,000 to 500 infringing copies.[**378]

Others noted the differing standards for proving infringement in China are hindering effective enforcement. They claim if something is not identical, even if confusingly similar, the Chinese government will not enforce the violation.[379] Critics allege counterfeiters are creating items very similar to the original protected item, but not identical, in order avoid enforcement.[380]

China's policy allows companies to file "bad faith" trademarks.[381] In the United States, a company may only file for a trademark it intends to use within 60 days. There is no such restriction in China. As a result, Chinese entities will register trademarks in China that the original creator of the trademark registered and uses in the United States. When the United States company seeks to operate in China, it must either purchase the trademark from the company that registered it or pay a licensing fee for its use.[382]

Rights holders and government officials both reported they would like to see true partnerships and joint investigations between the Ministry of Public Security in China and United States law enforcement.[383] United States government officials reported MPS will work with United States law enforcement when Chinese issues are at stake, but they are not true joint investigations. For

[*] These earlier thresholds required 500 items or the equivalent of approximately $7000 worth of counterfeited goods. See, Kevin Noonan, "WTO Panel Rules for U.S. in Chinese Copyright and Trademark Infringement Complaint, Patent Docs," 27 Jan. 2009. For many goods the dollar threshold is difficult to reach. For example, if the manufacturer reports that the cooling fan in a CPU only cost four cents to make, then it is extremely difficult to have sufficient products to make the monetary minimum. See Industry interview. Further complicating the threshold issue is a complaint that the police bureaus require proof that the threshold is met before they will investigate a case. See IIPA, "IIPA's 2010 Special 301 Report," People's Republic of China, 89.

[**] The USTR recently reported, however, that in May 2010 China "tripled the threshold for investigating and prosecuting trade in counterfeit products." See USTR, "2011 Special 301 Report," 21.

example, in an investigation targeting counterfeit software in China, Chinese authorities conducted seizures and arrests at a United States law enforcement agency's request, but the seized evidence was never shared with the United States law enforcement agency.[384] However, MPS has provided tips to CBP, such as one regarding a shipment of counterfeit Nike shoes. This tip led to a seizure of $45 million worth of counterfeit shoes.[385] MPS reported its priorities are: protection of the health and safety of Chinese consumers; protecting the rights of companies, both foreign and domestic; and working with foreign agencies.

Officials also reported corruption of Chinese officials made joint investigations difficult.[386] Corruption is a well-documented problem in China's government. Transparency International, a global organization focused on corruption issues around the world, gave China a score of 3.5 out of 10 (the lower the score, the higher the level of corruption).[*387] Chinese officials attending the Chinese Communist Party Central Party School listed corruption as either the most serious or second most serious social problem. Twenty-three percent of them listed local officials as "bad," and 12 percent concluded they were "very bad."[388] An average of 6,000 senior local officials were prosecuted for corruption each year from October 1997 to September 2007.[389] China's chief drug regulator was found guilty of taking $1 million in bribes "for approving more than a thousand drugs, many of them of dubious effectiveness and six of them outright fakes."[390] One commentator reported local officials "routinely protect Chinese counterfeiters in exchange for bribes."[391]

6. Addressing the problem

United States companies have adapted how they operate in China in response to the IPR environment. Some have increased their operations while others ceased. Others are working to change the Chinese views on the cost/benefit calculation of counterfeiting operations. For example, Intel initially refused to put any of its chip production plants in China because it was too risky due to the lack of IPR protections.[392] In 2010, however, Intel opened a fabricating plant in Dalian, China. It does not produce the latest generation of Intel's chips, only ones that have been on the market for some time and presumably could already have been reverse engineered. Other companies have decided to cease operations in China due to the lack of IP enforcement, moving manufacturing facilities to Vietnam or the United States.[393]

China Customs has increased its inspections of goods exported from China, providing evidence of some progress. A representative of the pharmaceutical industry noted China Customs has increased seizures of counterfeit pharmaceuticals from 470 shipments (256,972 tablets) in 2008 to 7,657 shipments (3,275,226 tablets) in 2009.[394] In 2010, China Customs seized over 100,000 counterfeit luxury goods discovered in nine containers.[395] China Customs has also adapted to changing shipping techniques. China Customs reports seizing 2.6 million infringing items[**] from postal and express consignments in the second half of 2009.[396] A United States foreign law enforcement partner reported having some successes with China Customs conducting controlled deliveries of counterfeit drugs.[397]

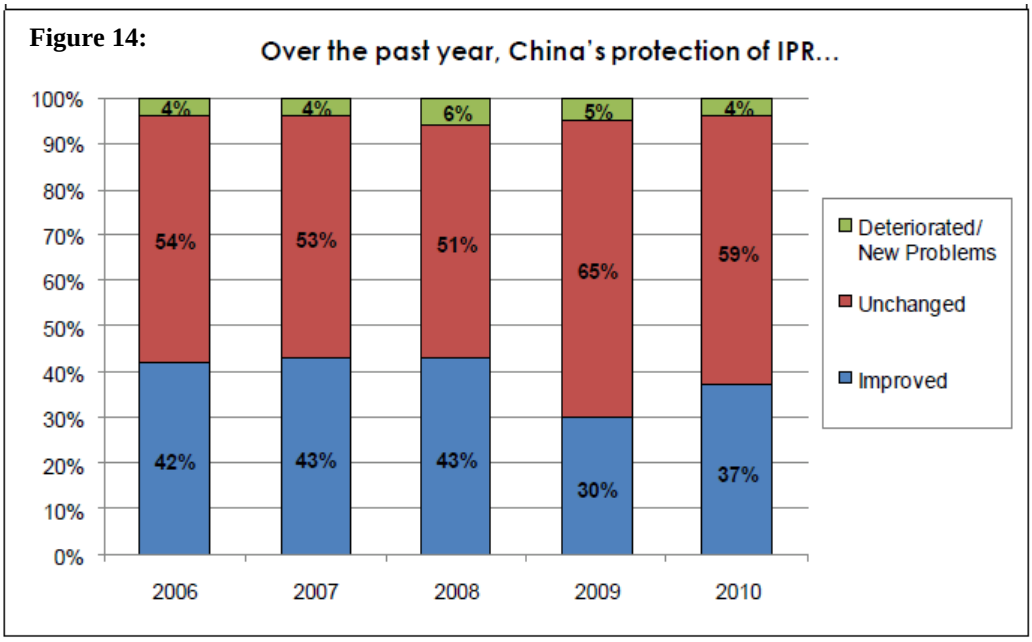
[*] In contrast, the United States was number 22 with a score of 7.1.

[**] It is not known whether these represent 2.6 million packages or individual items within packages.

Industry representatives also reported increasing numbers of administrative actions in China last year. One person reported having zero administrative actions in China in 2008 related to his company's trademark, 20 in 2009, and 30 in 2010. He is hopeful there will be 80 administrative actions and four to five criminal cases in 2011.[398] These administrative actions were worked jointly with China's MPS (Ministry of Public Security) and AIC (State Administration for Industry and Commerce). However, industry representatives explained China's law enforcement organizations do not always work well together. They contend the Shanghai Public Security Bureau (PSB) – the local police –work well with the AIC, but these organizations do not work well in other cities.[399] China's preference for administrative actions frustrated other industry representatives who wanted to see more criminal cases.

The United States China Business Council stated "China has made progress in recent years by improving its legal and regulatory IPR framework and by making uneven and gradual improvement in IPR enforcement but remains 'a major concern' for United States companies operating in China."[400] Its survey reported 37 percent of its members believe there has been some level of improvement in IPR enforcement in China in 2010. This statistic was an increase from the prior year but still lower than the highest years. Four percent indicated IPR enforcement deteriorated, and the remainder saw no change.[401]

Figure 14:



Source: The U.S.-China Business Council, "2011 Special 301 Review," 15 Feb. 2011.

Cases involving pirated content on websites demonstrate the continuing unevenness of IPR enforcement. In two cases China courts found infringement by websites that, though they did not keep infringing content on their servers, provided links for visitors to the website to click on to go directly to where they could obtain infringing content. The courts deemed they were facilitating and encouraging the illegal behavior.[402] These two cases did not sway the court that decided the Baidu case, which had essentially identical material facts, but came to a different conclusion. Some observers suggested the court in Baidu was influenced by the prominence of Baidu in China, which has been described as the "Google of China."[403]

Officials and courts are beginning to recognize the importance of protecting IP as more Chinese owned IP is being created. One observer noted that at a meeting of rights holders with local officials, the local officials were uninterested until a Chinese national spoke about infringement of her company's IPR. The officials then began to engage and be interested in the issue.[404] This recognition is expected to improve with the increasing sophistication of Chinese-owned companies regarding their IP rights. Moreover, it is expected that as Vietnam and Indonesia increasingly counterfeit Chinese goods and sell them at a lower price, China's law enforcement will be willing to be more active in IPR enforcement and work more joint investigations with foreign partners.[405]

There are now more cases in China's courts involving Chinese versus Chinese complaints than foreigner versus Chinese complaints, which is expected to have a significant impact on the willingness of local courts to enforce IPR.[406] Some have already noted they are "seeing some traction" in the courts. For example, the courts have begun to find for the plaintiffs in IPR cases and assess penalties.[407]

IP protection in China should continue to improve as it is expected that Chinese owned IP will grow steadily. China currently has 46 companies on the Global Fortune 500 list.[408] Major companies like Huawei, who once counterfeited Cisco products, are finding their own products counterfeited.[409] Chinese industries need to believe they have their own IP interests to protect.[410] Regardless of the level of efforts, this issue remains a cultural issue – because, as industry and government representatives agreed, counterfeiting is institutionalized as a way of life in China.[411] Some experts argue the most significant challenge for the Chinese government will be getting its citizens to realize what IP is and what activity is legal.[412]

The United States government is making efforts to improve the IP environment in China. For example, in October 2010, Attorney General Eric Holder traveled to Beijing, China, where he had a number of meetings with senior law enforcement officials including the Minister of Public Security to stress the importance of IP enforcement and bilateral cooperation between the U.S. and China. In addition, in September 2010, ICE Director Morton signed a letter of intent with China's MPS Director General Meng Qing-Fing to work together to combat IP theft and money laundering.[413] The Department of Justice's Criminal Division and the Ministry of Public Security's Economic Crime and Investigation Department co-chair the IP Criminal Enforcement Working Group (IPCEWG) of the U.S.-China Joint Liaison Group for Law Enforcement Cooperation (JLG). The IPCEWG is designed to increase information sharing and enhance law enforcement cooperation on intellectual property investigations and prosecutions. In addition, during a December 2010 meeting of the Joint Commission on Commerce and Trade (JCCT), the Chinese agreed to several notable efforts to improve the IP environment in China. They agreed to a multi-pronged program to ensure Chinese government offices use legal copies of software, including a pilot program involving 30 major state-owned enterprises.[414] The Chinese judiciary is drafting a Judicial Interpretation to combat online copyright infringement, including clearly stating those who facilitate online infringement will be liable for such infringement. In order to protect trademark rights in local markets, the judiciary has agreed to take legal measures to clarify the responsibilities and liabilities of market managers, landlords, and operators to supervise and inspect the activities of sellers in the markets.

It is important to improve the United States government's efforts to improve the protection of rights holders in China. Rights holders and government personnel who were interviewed by the TDY China Team concurred that the current United States government's efforts to address IP issues in China are "disjointed" and "ineffective."[415] The team was told that until the United States government demonstrates to the Chinese government that the United States is serious about IPR, enforcement in China would remain low.[416] The United States Ambassador in Beijing during the time of this review placed IPR in his top three priorities and held roundtables around China to raise the profile of the issue.*[417]

Some rights holders have suggested the United States government should focus its efforts on health and safety matters in China because they believe the Chinese government officials share those concerns and will be more motivated to work collaboratively to address such concerns.[418] It was reported that after milk containing melamine led to the deaths of children in China – although itself not an intellectual property violation – Chinese officials boosted their health and safety efforts.[419] Despite this improvement, United States officials were not able to obtain MPS cooperation on a criminal investigation into the case of the counterfeit Colgate toothpaste, which was contaminated with glycol, a principal ingredient in antifreeze. One United States government official noted his frustration with his inability to have a meeting with the prosecutors in China.[420]

Although the threat to United States rights holders and other United States interests from China-based IPR violations remains high, there are observable trends on the policy and enforcement fronts that may indicate a possible turning point. Commentators have noted as recently as the mid-1990s, United States rights holders faced similar problems in Japan. Once Japan began to create its own IP that it valued protecting, the IP environment in Japan changed. Now Japan is considered an excellent IPR enforcer.[421] This change suggests that as China moves forward in developing its own IP and begins to experience a cultural shift valuing its protection, the current threat may be mitigated.

B. India

India-based IPR infringement, particularly counterfeit pharmaceuticals, content piracy, and automobile parts, poses an economic threat to United States IP interests. India-sourced counterfeit pharmaceuticals and automotive parts shipped to the United States also pose a health and safety threat to United States consumers.[422] Despite noting some progress, the United States Trade Representative continued to place India on its 2011 Priority Watch List due to concerns regarding India's "weak legal framework" and persistent "ineffective" IPR enforcement.[423]

Source: CIA World Factbook

* The ambassador has departed and it is uncertain what the new ambassador's priorities will be.

1. Background

With a GDP (based on a purchasing power parity basis) of $4 trillion in 2010, India is the fourth largest economy in the world. Its population of 1.2 billion makes it the second largest potential market for goods and services in the world, only slightly trailing behind China. Although its middle class population – currently believed to be around 50 million – is significantly smaller than China's, it is estimated to grow tenfold by 2025.[424] It is the fourteenth largest exporter to the United States, with $29.5 billion worth of goods flowing to the United States in 2010.[425] Pharmaceuticals accounted for $3.2 billion and automotive parts for $810 million of these goods.[426]

2. The nature and magnitude of the threat

There is no way to measure accurately the total amount of infringing goods shipped to the United States from India because it is not possible to know the amount of infringing goods that are not seized. The only available indicator is CBP and ICE seizure statistics. In 2010, CBP and ICE conducted 79 seizures of goods shipped from India with a domestic value of approximately $1.6 million. As depicted in Figure 15, the 2010 seizures declined in number and value from 2009.[*] The number of seizures from India peaked in 2009 but the value of such seizures peaked in 2008. These figures do not indicate a definite lessened threat from infringing goods from India. The statistics report CBP and ICE's seizures from each year. One or two particularly large seizures of a particular type of good or in a particular country may skew the figures.

Figure 15:

India's Share of CBP Annual Seizures

Fiscal Year	Number of Seizures	Percentage of Seizures	Domestic Value
2010	79	< 1	$1.6M
2009	279	1	$3.0M
2008	170	6	$16.2 M
2007	N/A	< 1	$0.9M
2006	N/A	< 1	$0.8M

Source: U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, "Intellectual Property Rights Seizure Statistics," Fiscal Years 2006-2010.

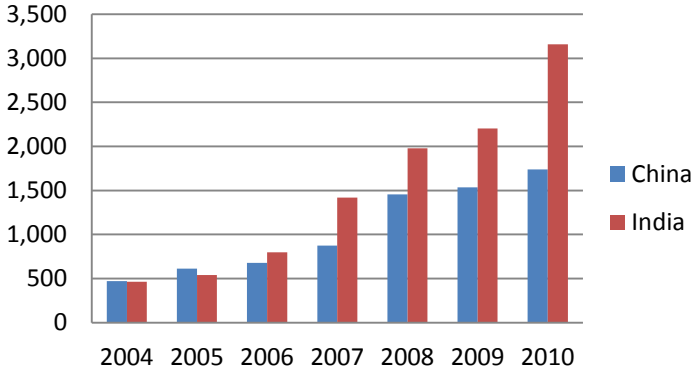
Contrary to the infringing environment in China, reporting indicates a significant portion of counterfeit goods distributed in India are not manufactured there. Several industry representatives and government officials interviewed by the TDY India Team explained offenders in China manufacture infringing goods, such as counterfeit pharmaceuticals and automotive parts, and ship them to India for distribution and local consumption.[427] It is possible a portion of the infringing goods entering the United States from India originated in China, but distributors transshipped them via India.

[*] China and Hong Kong were responsible for the first and second largest percentages of IPR seizures by domestic value, respectively. See U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, "Intellectual Property Rights Seizure Statistics," Fiscal Year 2009, 2010.

Pharmaceuticals

The Indian pharmaceutical industry is the third largest in the world producing $21.26 billion worth of pharmaceuticals between 2009 and 2010.[428] Although experts believe India residents consume the majority of pharmaceuticals produced in India, India still exports significant quantities of them.[429] As seen in Figure 16, in 2006 India surpassed China in terms of the value of declared imports of pharmaceuticals into the United States. From 2006 to 2010 India's pharmaceuticals exports to the United States grew nearly 400 percent.[430]

Figure 16: United States Pharmaceutical Imports 2004-2010 (millions of dollars)



Source: U.S. Census, "U.S. Imports from India by 5-digit End-Use Code Data," 2002-2010.

Without a corresponding shift of known legitimate production, the rapid increase in shipments from India may indicate a growing problem of counterfeit pharmaceuticals from offenders in India.* Views regarding the size of the threat from counterfeit Indian pharmaceuticals vary.** Many still identify China as the principal source of counterfeit pharmaceuticals, but others say India quickly is approaching China's production levels. One individual believes India has overtaken China as the principal source for counterfeit pharmaceuticals.[431]

One government official believes most of the pharmaceuticals produced in India are copies of patented drugs but do not bear the trademark of the patent holder.*** He contended counterfeit drugs that are not "generic" are from China, and counterfeiters sometimes use India as a transshipment point.****[432] The IPR Center did not locate any statistical evidence to either support or refute these contentions.

* An alternative explanation might be a substantial increase in the amount of pharmaceuticals transshipped from China through India to the United States. Some evidence indicates this transshipment is occurring, but there are no known measures for such activity. Further investigation of these trends is needed to make concrete conclusions regarding the source of these shifts.

** Understanding the issue in India is complicated by the variety of terms used to describe the various pharmaceuticals produced there, including "counterfeit," "misbranded," "substandard," and "spurious." These terms distinguish pharmaceuticals from generic versions of patented drugs that India allows but the United States does not. The term substandard is used most frequently but may refer to any poor quality drug. Substandard drugs are a large problem in India but the term covers a broader range of products than just counterfeit.

*** These drugs are the equivalent of generics but are made in violation of the patent holders' rights because they are still covered by legitimate patents.

**** Some open source reports give examples of drugs being labeled as made in India but actually were made in China. See, e.g., Rama Lakshmi, "India's market in generic drugs also leads to counterfeiting," *The Washington Post*, 11 Sept. 2010.

India's share of CBP and ICE's pharmaceutical seizures in 2008 was 58 percent, but fell to 24 percent for both 2009 and 2010.[433] These variations in percentages may be due to a number of factors, such as targeted operations or how products are being shipped, unrelated to what is actually shipped to the United States from India. Pharmaceuticals remain, however, the primary commodity shipped from India seized by CBP and ICE, accounting for 86 percent of the value of goods seized from India in 2010.[434] The majority of counterfeit pharmaceuticals entering the United States from India are believed to come via Internet sales.[*435]

The Indian government attempted to measure the quantity of counterfeit drugs in India. Its study reported only 0.4 percent of the drugs in the Indian supply chain are counterfeit. Experts claim the study was flawed because the researchers only examined the stock on shelves in legitimate licensed pharmacies.[436] Critics explained pharmacists store counterfeit drugs under the counter and only offer them to certain customers who cannot afford genuine drugs.[437] These pharmacies do not account for the sales of drugs on the Internet or through other locations. One independent study reported 3.6 percent of the drugs sampled from some Delhi wholesalers likely were counterfeit, and poorer areas of India will have higher numbers.[438] Another study estimates 15 to 20 percent of pharmaceuticals in the Indian market are counterfeit.[439]

Piracy

Content piracy in India satisfies Indian domestic demand but infringes on United States rights holders' interests. The physical music piracy rate in India in 2009 was estimated at 60 percent with losses of $17.7 million.[440] These statistics indicate a 50 percent decline in losses despite a 10 percent higher piracy rate from the prior year. As these figures only include physical piracy this shift may reflect movement to digital piracy for music. Business software piracy in India in 2009 was an estimated 65 percent, with losses of $1.5 billion (fourth highest in the world in 2009).[441] Although business software piracy rates declined slightly from the prior year, losses increased approximately nine percent during the same time period with a corresponding increase in personal computers. Estimates of film piracy rates and losses to United States film companies from movie piracy in India are comparatively low – a 29 percent piracy rate (ranking ninth worldwide) and less than $149 million in losses.[**] Although these industry generated figures may not be precisely correct, they do indicate a large problem.

MPA calculated movie piracy losses based on actual and lost sales in the legitimate movie market. These figures likely underestimate the actual prevalence of film piracy in India because of the limited market for legitimate American films.[442] A United States government official working in India explained legitimate movie theaters lowered admittance prices to approximately

[*] For example, in May 2010 two United States persons were convicted of selling unapproved and unbranded pharmaceuticals using an illegal Internet pharmacy. Although advertising brand name pharmaceuticals they filled orders with misbranded and unapproved drugs from India. See Department of Justice, "Kingman Couple Sentenced For Fraudulently Distributing Indian-Manufactured Counterfeit Drugs," *Press Release*, 25 May 2010.

[**] India was not one of the top ten countries for revenue losses from movie piracy, and as such the true value of the lost revenue was not reported (except that it was lower than the tenth ranked country, valued at $149 million). See MPA and L.E.K., "The Cost of Movie Piracy," 2008, 4.

one dollar, but people do not attend when they can view pirated content for less.[*443] Thousands of stores in India rent pirated videos at low prices, eliminating most of the rental market for legitimate products.[444] Raids in 2010 continue to recover large amounts of pirated content. For example, in Mumbai police seized over 84,000 pirated DVDs, 1,400 blank DVDs, and 42 DVD writers.[445] Three raids across India in May 2010 seized approximately 15,000 pirated DVDs each, as well as 19 DVD writers.

Although evidence indicates a global trend toward digitally delivered pirated content,[446] the majority of reporting indicates most pirated content in India is still distributed through burned discs sold at marketplaces.[447] These discs may contain pre-released music, movies, business software, entertainment software, and books or reference materials.[448] These copies are not sophisticated or made to appear genuine. Retailers frequently sell pirated discs in plastic bags and label the discs with black ink.[449] In addition to pirated content sold on optical discs, interviews with industry representatives in India indicate mobile chip piracy is becoming a popular method of increasing cellular phone sales and distributing pirated content.[450]

Automotive parts

Evidence regarding counterfeit automotive parts from India is anecdotal, although industry representatives report it is an issue.[451] According to a 2007 study sponsored by the Society of Indian Automobile Manufacturers (SIAM) and the Automotive Component Manufacturers Association of India (ACMA), the value of counterfeit automotive parts sold within India each year equals between $1 and 1.3 billion.[452] According to one United States government representative, India is second behind China for producing counterfeit automotive parts seized by CBP and ICE.[453] CBP and ICE annual statistical summaries do not report counterfeit automotive parts seized in the United States from India because these items did not meet the reporting threshold. This suggests counterfeit automotive parts are a low volume threat, although the harm these items may cause is high.[454]

Little information exists about how manufacturers produce these parts and distribute them to United States consumers. One industry representative cited a warehouse located in the United States belonging to a New Delhi-based distributor of counterfeit automotive parts as evidence of these parts entering the United States.[455] The IPR Center found no statistical evidence of the threat to United States consumers; therefore, the magnitude of this threat remains unknown.

3. Offenders

Although individual offenders may be responsible for the majority of the IPR violations affecting United States interests in India, the offenders of principal concern have been those associated with formal criminal networks. As described in Section VI of this report, Dawood Ibrahim's D-Company is involved in film piracy and other criminal activity. The 2009 RAND study of film piracy reports D-Company vertically integrated itself throughout the pirated film business since the 1980s, "forging a clear pirate monopoly over competitors and launching a racket to control

[*] Recent industry reports of box office sales indicate this trend is beginning to turn with the rapid growth in the size of the middle class in India who are beginning to go to see films in theaters. See William Smale, "Downturn gives Hollywood bad dreams," *BBC News Business,* 17 Feb. 2011, http://www.bbc.co.uk/news/business-12460222.

the master copies of pirated Bollywood and Hollywood films."[456] Ibrahim also has ties to terrorism.[457] Due to a lack of visibility into D-Company's finances, the IPR Center cannot directly link D-Company's piracy revenue to terrorist financing. Moreover, as noted previously, evidence of this particular threat is dated and it is likely to have changed significantly in the past decade.

4. Enforcement environment

Industry and government officials cite corruption as a significant enabler of IP theft in India. Police, pharmacists, and pharmaceutical inspectors reportedly took bribes, dispensed unauthorized pharmaceuticals, and produced fake laboratory reports indicating industry-identified infringing pharmaceuticals were authentic.[458] Transparency International ranked India 87 out of 178 countries (the higher the ranking number, the higher the level of corruption) and earned a score of 3.3 for corruption, indicating there is slightly more corruption in India than China.[459]

Police, judges, and the public in India do not perceive IPR enforcement as a national priority. Other priorities, such as poverty and insufficient medical care, outweigh concerns for IPR.[460] There are insufficient laws to protect IP, and law enforcement inadequately enforces laws that do exist.[*] Lenient sentencing further undercuts enforcement. Few criminal sentences are imposed for IPR violators. One United States government official cited an example where an IPR violator received a one-day sentence with credit for time served in court that day. Such leniency further discourages spending time and effort on IPR enforcement.[461]

Interviews with government officials and industry representatives indicate the High Court is the only court that addresses IPR matters. There is a complex structure of local police and metropolitan magistrates that complicate IPR prosecutions. Insufficient police resources, prosecutors inexperienced in prosecuting IPR matters, long delays, and conviction rates as low as two percent, are considered the norm in Indian courts, especially in the case of pharmaceuticals.[462]

Several other issues complicate IPR enforcement in India. For one, most enforcement agencies do not computerize or consistently maintain their records. There are few national databases and no interstate records that can tell police in one state that a person has a record or is wanted in another state. One government representative gave an example of seeking a customs document from Indian officials and the officials responded nine months later, explaining a flood ruined all the documents.[463] Several individuals reported the police are poorly trained and when conducting raids they may seize infringing goods but none of the relevant business records.[464]

5. Addressing the problem

The 2011 Special 301 Report noted India has made "incremental improvements" in IPR enforcement. It encouraged India to improve its criminal enforcement by increasing "the efficiency

[*] The OECD noted that the weaknesses that counterfeiters often exploit are lack of legislation, regulation, enforcement, and punishment. See Organisation for Economic Co-Operation and Development, "The Economic Impact of Counterfeiting and Piracy," 2008, 370.

of judicial proceedings," "encouraging the imposition of deterrent-level sentences for IPR violations," and "giving prosecution of IPR offenses greater priority."[465]

With the assistance of the United States government and industry, the Indian government is taking action on several fronts to address the IP problem. For example, the United States government is working with India to establish a "camcording law" to protect against immediate distribution of first-run movies.[466] The USPTO is using outreach and education in India for Indian police, judges, and customs officials regarding enforcement of international laws and regulations, as well as identification of infringements.[467] The Indian government established an Intellectual Property Training Institute (IPTI) to educate and training professionals and the wider public.[468] The United States Department of Justice has been working with the High Courts in Delhi and Bangalore to implement specialized court programs to facilitate and speed up the process for IP cases. It has also been involved in training judges and prosecutors in IP matters.[469]

India has increased the number of courts handling IPR crimes, and made some recent changes in laws. For example, a person convicted of producing counterfeit pharmaceuticals may receive a life sentence. Under a new pharmaceutical whistleblower policy individuals can contact authorities with information regarding IP theft. The authorities will maintain their confidentiality and they are eligible for a $50,000 reward.[470] The number of people arrested in India for selling counterfeit drugs rose from 12 in 2006 to 147 in 2009.[471]

C. Russia

Russia-based content piracy poses an economic threat to United States IP interests, but United States consumers are at little risk from infringing goods originating from Russia. Despite noting some progress, the United States Trade Representative continued to place Russia on its 2011 Priority Watch List due to "ongoing concerns, particularly with respect to privacy over the Internet and enforcement generally."[472]

Source: CIA World Factbook

1. Background

Russia's Gross Domestic Product (based on a purchasing power parity basis) was $1.477 trillion in 2010.[473] Its current population is 139.4 million but is declining.[474] In 2010, Russia exported $25.968 billion worth of goods to the United States. Although it is the sixteenth largest exporter of goods to the United States, it only accounted for 1.3 percent of imports in 2010.[475] Eighty-eight percent of the goods the United States imported from Russia were either fuels (including crude oil, fuel oil, and nuclear fuels) or various metals.[476]

2. The nature and magnitude of the threat

Consistent with other sources of information, the USTR Special 301 Report indicates piracy of United States copyrighted media is the most significant threat from Russia to United States IP interests. Although the USTR report notes rights holders' complaints regarding counterfeiting of "consumer goods, distilled spirits, agricultural chemicals, biotechnology, and pharmaceuticals,"[477] the IPR Center found little evidence that Russia exports significant quantities of these goods to the United States.

A 2006 industry report claimed filmmakers lost 79 percent of their potential market in Russia to piracy, the second highest rate in the world. As a result, filmmakers estimate they lost $266 million of revenues in Russia, the fourth highest revenue losses in the world.[*478] Pirates most often obtain film content via camcording in movie theaters. According to the IIPA, Russia is the world's leading source of illicit full-video recordings of films from theaters.[479] Individuals illegally recorded seventy-five full length films in Russian theaters in 2010, almost double from the prior year.[480] Since 2009, authorities stopped 61 people from recording movies in Russian theaters.[481]

Optical disc piracy, while less common due to the increasing availability of pirated content on the Internet, is still significant in Russia. IIPA identified Russia as one of the top two "optical disc piracy factory production trouble spots" in 2009.[**482] According to the Russian police, thieves pirated approximately 70 million discs in 2009, with an estimated retail value of $630 million.[483] According to the IIPA, the United States government estimates at least 30 optical disc plants remain in operation in Russia in 2009.[484] In 2010, authorities raided 11 pirating warehouses, resulting in seizures of over 10 million pirated discs.[485]

Internet piracy continues to grow, despite the closing of several illegal websites offering pirated content.[486] For example, the Russian government shut down allofmp3.com, the largest P2P network in Russia (based on downloads), in 2007 due to large-scale copyright infringement. Thirty digital piracy websites with similar business models replaced allofmp3.com since its removal.[487] IIPA reports Russian online social network vKontakte "is the largest single distributor of infringing music in Russia and one of the largest in the world."[488] The USTR includes vKontakte on its list of notorious markets.[489]

Although Russia's software piracy in 2010 was 1 percentage points lower than in 2005, it still was 67 percent.[490] Business software piracy in Russia cost United States companies approximately $1.869 billion in 2009, second only to China in losses in foreign countries.[491] The Entertainment Software Association (ESA) reports video game piracy remains high. ESA estimated in December 2009 alone, Russian members of P2P networks made 118,211 infringing copies of ESA members' computer and video games.[***492]

---

[*] Although these numbers are not specific to the United States, a significant portion of MPA members and movies are United States interests, implying corresponding rates of piracy and financial losses apply to the United States film industry.

[**] China was the other identified country.

[***] These figures do not account for cyberlockers or "one-click" hosting sites, which would increase the number of infringing copies.

3. Offenders

The two types of Russian IPR offenders of most concern to United States interests are warez groups and criminal enterprises. Warez groups are responsible for online piracy. Russian warez groups have provided copies of movies that were still in theaters to a warez group based in the United States, which in turn digitally distributed the video content.[493]

As described in Section VI of this analysis, Russian criminal enterprises are involved in IP theft. The reporting indicates Russian criminal enterprises involved in IPR violations are involved most often in content piracy.[*494]

4. Enforcement environment

The IIPA reported overall the Russians have made progress against physical piracy and contends Russia has adequate enforcement mechanisms for addressing the physical piracy problem. IIPA complains, however, the number of enforcement actions is declining and the Russians have taken little action to address Internet piracy.[495]

According to a United States official working in Russia, corruption within Russian law enforcement and policy organizations is the largest obstacle to Russia's effective enforcement of IPR. For example, the official explained much of Russia's seized infringing goods are not properly disposed of and "vanish" from warehouses.[496] Raid plans for optical disc production facilities have been leaked to plants in advance, decreasing the chances of finding counterfeit discs and minimizing potential evidence to pursue charges.[497] Transparency International gave Russia gave Russia a score of 2.1out of 10, indicating there is substantially more corruption there than in either China or India.[498]

In Russia, the government cannot hold a business corporation criminally liable for any actions, including IPR infringements.[499] There is evidence of Russian companies appointing a "fall guy" who they publicly designate as head of a company. These "fall guys" assume criminal liability but law enforcement cannot take actions against the corporation.[500] Copyright industries report criminal penalties and sanctions are inadequate and do not provide deterrence. It is rare for the Russian government to impose criminal penalties on website owners conducting Internet piracy.[501]

A United States government official believes Russia currently lacks the resources and funding needed to enforce existing IPR laws. The official believes Russia needs to increase the prioritization of IPR enforcement to successfully obtain membership in the WTO and grow Russia's overall economy.[502] The investigation process may need improvements as observers cite the length of piracy investigations as a reason for the decline in the number of criminal actions taken in the past two years.[503]

[*] Refer to Section VI for more analysis about the specifics of Russian criminal enterprises involved in IPR violations.

5. Addressing the problem

Russia made several improvements in its attempts to enforce IPR violations. There is increased enforcement against optical disc piracy, including a 2008 ban on cameras in theaters and a ban on selling pirated optical discs in the underground metro systems.[504] Russia's Federal Service for Intellectual Property, Patents and Trademarks (Rospatent), established patent chambers to adjudicate patent and trademark disputes.[505] Rospatent, through the establishment of the Russian State Educational Institute for Intellectual Property, offers courses, seminars, and workshops to industry members and the general public.[506] Sales of legitimate media discs are rising in Russia. Increased enforcement actions are cited as the cause of this increase.[507] Movie theater revenues have increased.[508] The expanding middle class in Russia is cited as the cause of this improvement.

D. Tri-border Area of South America

The TBA is considered a "safe-haven for groups engaged in the illicit manufacture, transshipment, and sale of counterfeit goods and pirated digital content."[509] The USTR placed Argentina on the Special 301 Priority Watch List, Brazil on the Watch List, and Paraguay under Section 306 Monitoring primarily because of internal IP concerns, particularly ineffective prosecutions of and non-deterrent sentences for IPR violators.[510] The USTR judged that, with the exception of digital and physical piracy of multimedia content, the TBA does not pose a significant threat to United States interests. The principal concerns with this region are the piracy of United States rights holders' protected content and the financing of criminal and/or terrorist organizations with funds earned from IP theft.

The TBA is the intersection of Argentina, Brazil, and Paraguay

Source: "Hezbollah Builds a Western Base," http://www.msnbc.msn.com/id/17874369/ns/world_news-americas/

1. The nature of the threat

Physical and online piracy of multimedia content are the most common infringing goods in the TBA, although counterfeit electronic devices, pharmaceuticals, pesticides, and aircraft parts also may be found there.[511] The majority of these infringing goods are consumed in the local South American market, particularly Brazil. Individuals in Brazil may turn to counterfeit goods to avoid Brazil's extremely high import taxes.[512]

Although there is evidence of transshipment of infringing goods within the TBA,[513] this evidence does not indicate the TBA is a significant transshipment place for goods coming to the United States. Together the TBA countries are responsible for less than two percent of all United States imports and the majority of these imports are fuel related or ores.[*] CBP and ICE reports of

[*] Brazil accounts for approximately 1.02 percent of U.S. imports, Paraguay and Argentina each account for less than 1 percent of U.S. imports.

seizures of infringing goods from the TBA countries are consistent with this conclusion. During FY 2010, ICE-HSI and CBP made three IPR seizures of goods from Argentina, two from Paraguay, and eight from Brazil.[514]

Counterfeit aircraft parts imported from Brazil are a potential exception to this finding of low risk of infringing goods coming to the United States. Between 2002 and 2010, the United States imported over $15 billion worth of civilian aircraft and aircraft parts from Brazil.[515] A review of reported counterfeit aircraft parts between June 2008 and November 2009 determined that at least 6 percent of these parts originated overseas. China, Brazil, and Mexico were the leading suppliers of these counterfeit parts, but the origin of many of the parts was never determined. Moreover, as noted earlier, many counterfeit parts are never reported to the FAA or GIDEP. Based on these factors, it is likely more counterfeit aircraft parts from Brazil entered the United States supply chain. As the types of goods seized from Brazil do not meet the reporting threshold for CBP and ICE annual seizure reports, no additional evidence of counterfeit aircraft parts being shipped to the United States from Brazil was located.

2. The magnitude of the threat

The impact on United States rights holders from IP theft in the TBA is unknown. There has not been a systematic analysis to determine the portion of goods in the TBA that infringe upon United States rights holders' IPR. Anecdotal evidence from United States government personnel working in the TBA and local open source reporting indicate there is some. There are some estimates of losses to United States interests from various forms of piracy. IIPA reported that in 2009 Argentina had a 60 percent physical music piracy rate and Brazil had a 48 percent rate with corresponding losses of $63.4 million in Argentina and $147 million in Brazil.[516] IIPA reported that in 2007, the last year for which there was data, Paraguay had a 99 percent physical music piracy rate with corresponding losses of $128 million.[*517] IIPA also provided estimates of losses from piracy of business software in 2009. Paraguay had the highest piracy rate of the three countries – 82 percent – but estimated losses of only 8 million. In contrast, Argentina's piracy rate was 71 percent with losses of $209 million. Brazil's piracy rate was 56 percent with corresponding estimated losses of $831 million.

3. Offenders

As discussed in Section VI, terrorist supporters have used IP crime as one method to raise funds for terrorist organizations. The TBA is one of the main fundraising locations for Lebanese Hizballah, a designated terrorist organization. Hizballah supporters in the TBA use profits earned from IP theft, particularly distributing pirated media content (CDs, DVDs, software), to provide financial support to Hizballah.[518]

[*] As there has been a significant movement from physical to digital piracy, the loss figures have declined from 2001 even though the piracy rates have remained the same. In addition, these figures include losses from transshipments so they likely double count some of the losses attributed to Brazil and Argentina.

For example, Assad Ahmad Barakat, Hizballah's chief fund-raising officer in the TBA, raised money by selling pirated software smuggled into the TBA from Hong Kong.[*] Another Hizballah supporter, Ali Khalil Mehri, was charged by Paraguayan authorities with "piracy of computer programs and CDs and with selling millions of dollars of counterfeit software and funneling the proceeds to Hizballah."[**][519]

Organized criminal enterprises in the TBA also are involved in IP theft alongside other criminal activities, including narcotics trafficking, weapons smuggling, and vehicle part theft.[520] For example, in January 2010, Brazilian authorities arrested 129 individuals involved in trafficking cocaine, operating clandestine mechanic shops, and burning pirated DVDs."[521]

4. Addressing the problem

Currently IPR violations in the TBA are addressed at the state level. According to a United States government official working in the TBA, there is little coordination between states within each country or between the three TBA countries.[522] Some efforts have been made by state police to improve their coordination, including holding IP conferences and working groups for the different law enforcement groups in the region. USPTO has an IPR Attaché in Rio de Janeiro, Brazil whose jurisdiction includes the entire TBA region. Brazil also has an Intellectual Property Action Plan to help address IPR concerns in the region.[523]

In Brazil some laws exist to provide severe penalties for IPR violations. For example, the penalty for manufacturing and selling counterfeit pharmaceuticals can be as high as 10 to 15 years in prison and fines up to $2 million. However, there is no evidence of individuals being imprisoned or fined with these maximum sentences from IPR violations. In some cases, local drug gangs control parts of the larger cities, preventing IPR cases from being prosecuted.[524]

A principal reason for focusing on IPR violations in the TBA is the potential for terrorist financing from IPR violations. Collaboration with local law enforcement regarding this issue can be difficult because the United States considers Hizballah a terrorist organization but the countries in the TBA do not. Local law enforcement agencies may collaborate with United States agencies on IPR matters if the investigation focuses solely on the IPR crime, not potential terrorist financing from the crimes.[525]

E. United States of America

The USTR does not evaluate the domestic threat to United States rights holders' IP. Although the majority of infringing physical goods consumed in the United States are manufactured overseas and imported into the United States, there are significant domestic IPR violations. These violations include extensive piracy of copyrighted music, movies, and software, some manufacturing of counterfeit goods, and extensive distribution operations for imported infringing goods. In addition, theft of trade secrets from United States companies is most often committed within the United States by United States offenders. This section will focus on IPR violations

[*] Although this reporting is dated (early 2000s), it provides concrete examples of IPR violations in the TBA funding Hizballah.

[**] Mehri fled the country to avoid further imprisonment.

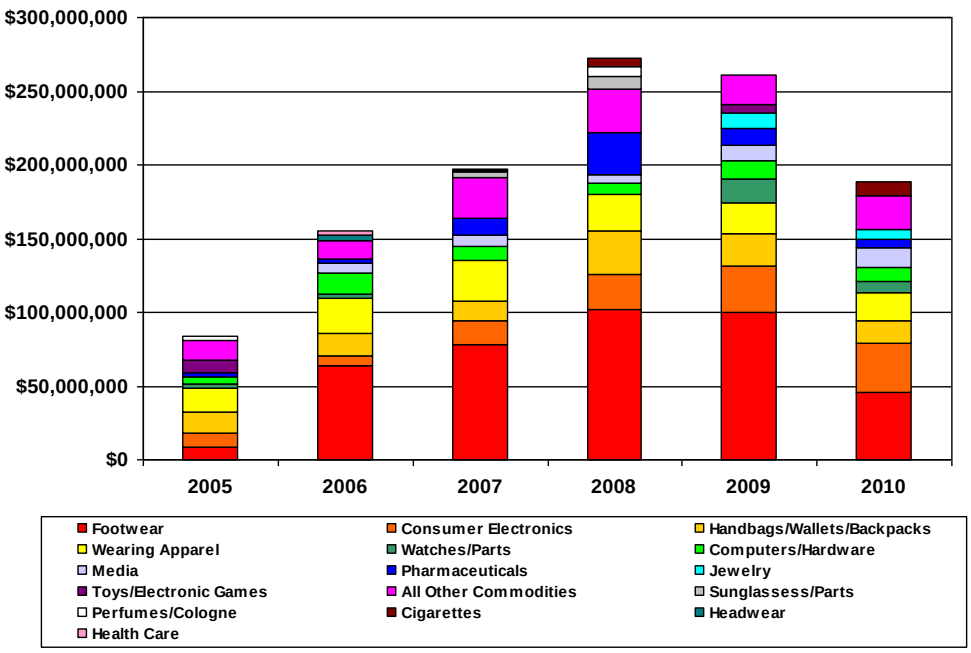
specifically involving offenders within the United States.

Source: CIA World Factbook

1. The nature of the threat

Except for piracy, both physical and digital, the majority of infringing goods seized in the United States are imported from other countries, principally China. There are numerous types of goods coming to the United States; 600 different categories of infringing goods have been seized in the United States.[526] Counterfeit footwear, consumer electronics, clothing, and clothing accessories (e.g. watches, handbags, wallets, etc) are the most often seized categories of goods. As seen in Figure 17, these categories accounted for over 50 percent of all infringing goods seized by CBP and ICE-HSI each fiscal year from 2005 to 2010. Seizures are not necessarily representative of the percentages of types of infringing goods actually present within the United States but these figures provide insights into the infringing goods being shipped to the United States.

Figure 17: Domestic Value of United States IPR Seizures by Category, FY 2005-2010



Source: U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, "Intellectual Property Rights Seizure Statistics," Fiscal Years 2005-2010.

Production of infringing goods in the United States

There are no analyses of the amount of infringing goods manufactured or finished in the United States but anecdotal evidence from criminal investigations indicates it occurs. Seizure statistics from other countries indicate low levels of infringing goods are shipped from the United States. These statistics suggest the United States is not a major producer of infringing goods. It is, however, a significant consumer of such goods. As a result, there are considerable distribution and sales networks for transporting and selling imported and domestically produced infringing goods in the United States.

Low levels of infringing goods are manufactured domestically in the United States. The most significant domestic manufacturing operations of infringing goods involve pirated music and movies. The relatively lower levels of domestic physical production of infringing goods are driven by two key factors: profitability and risk. Counterfeiters balance these two factors to determine whether it is more profitable to produce an infringing good within the country where it will be sold or to produce it elsewhere and risk potentially having the goods seized during importation.[527] For non-media goods, evidence indicates most operators will manufacture the infringing goods overseas and import them into the United States. Media goods are the principal exception, as the costs of manufacturing pirated discs are so low that it would be disadvantageous to have the discs manufactured overseas and shipped to the United States.[528] Furthermore, an analysis of CBP, FBI, and ICE press releases from 2008 to 2010 regarding seizures and prosecutions of counterfeit goods manufactured in the United States indicated 19 of the 26 reported cases (73 percent) involved pirated media content. This analysis was not a scientific study but nonetheless is consistent with a finding that pirated content comprises the majority of domestically produced infringing goods.[529] In addition to pirated media content, printing of sports apparel and paraphernalia for last minute sport events, such as the World Series or Super Bowl, is common in the United States because there is not enough time to import these goods from other countries.

There is isolated evidence of United States offenders domestically manufacturing infringing goods other than optical discs. Some examples include a small Miami-based operation manufacturing counterfeit military aircraft parts, counterfeit pharmaceuticals manufactured in Florida,[530] and counterfeit luxury goods assembled in California.[531]

Some portions of the production or assembly of infringing goods may occur in the United States. For example, unbranded clothing may be exported to the United States separately from infringing labels. The labels or other infringing marks, such as embroidery, will be applied to the items in the United States.[*] Several industry representatives in the electronics and technology industries reported cases of counterfeit labels being applied to generic goods after the goods were shipped into the United States.[532]

BASCAP figures regarding domestically produced infringing goods suggest 20 percent of the physical infringing goods in the United States are produced domestically. This figure is inconsistent with other evidence and likely overstates the amount of domestically produced

[*] Some countries are considering laws that would allow the seizure of unbranded goods if they are shipped with labels as it is clear they are intended to be transformed into counterfeit goods.

infringing goods. BASCAP noted these estimates were based on an assumption that "there is a strong relationship between the ratio of counterfeit products in a country's exports and the ratio of counterfeit products in its domestic production."[533] Yet other countries' seizure statistics do not support a finding that over 20 percent of the goods coming into that country from the United States was counterfeit.

Theft of trade secrets

A review of cases of thefts of trade secrets from United States rights holders revealed this theft most often occurred within the United States. United States offenders are most responsible for the domestic theft of United States intellectual property. Approximately 84 percent of the trade secret investigations examined had no known foreign nexus.[534]

Physical domestic distribution

There are several common distribution methods once infringing goods have passed customs and entered the United States. Individuals, sometimes acting on their own and other times acting on the behalf of wholesalers, may pick up infringing goods and sell them to other distributors. In other cases, distributors may transport the goods, either themselves or through commercial trucking companies, to another part of the country, typically from west to east. The hired trucking companies may or may not be aware they are transporting infringing goods.[535] The infringing goods usually are moved domestically via vans or trucks because this is more cost effective than air-shipping the goods. This shipping method is also perceived to reduce the risk of law enforcement discovering the goods. Infringing goods may be hidden by intermingling them with legitimate goods, such as placing counterfeit music CDs on trucks carrying produce from Los Angeles to New York.[536] Once the infringing goods reach their intended area of the country, they are distributed to individual retailers who may sell them in flea markets, stores, on street corners, and other similar venues. Canal Street in New York City and Santee Alley in Los Angeles are two of the most notorious markets in the United States for selling infringing goods.[537]

Individuals who are manufacturing, selling, and distributing their infringing goods may have more localized operations involving fewer individuals. For example, a South Carolina man manufacturing counterfeit Super Bowl clothing used his own screen printing equipment to manufacture the goods and personally took his counterfeit clothing to the Super Bowl venue to sell it.[538] Another individual bought active primary ingredients for various drugs, produced his own counterfeit pharmaceuticals, and then distributed them via the Internet.[539]

In other cases, individuals serve simply as brokers or intermediaries for sales between suppliers of counterfeit goods and end consumers. For example, individuals in the United States may import goods they purchase from overseas vendors, such as a website in China, and then repackage them for shipping via commercial services to customers, such as the United States military.[540]

Finally, consumers of infringing goods in the United States may bypass the traditional, controlled distribution methods by making purchases online or accessing pirated multimedia

content posted on the Internet. Although no systematic analysis of the number of purchases of infringing goods using the Internet has been conducted, reports from industry representatives and United States government officials confirm the high significance of the Internet as a mechanism for customers obtaining infringing goods.[541] Counterfeit luxury goods and clothing increasingly are being sold directly to United States consumers via websites. Representatives from the pharmaceutical industry cite the Internet as the most significant method for counterfeit pharmaceuticals to reach United States consumers.[542]

Exports of infringing goods to other countries

There are no reported domestic measures regarding infringing goods being shipped out of the United States. European Union statistics of infringing goods seized at its borders indicate the United States is the country of origin for some counterfeit goods. In 2009, the United States was the source of 26 percent (approximately 50,000 individual items) of the 190,951 infringing "foodstuffs, alcoholic and other beverages" items seized at a European Union country border.[*543] It is unknown what percentage of cases involving these items involved goods from the United States. It is also unknown whether the goods were manufactured in the United States or whether the United States was a transshipment point for the goods.

The European Union made seizures of goods from the United States in other years as well. In 2008, 1.93 percent of the counterfeit foodstuff and beverages, 1.43 percent of the counterfeit computer equipment, and 0.14 percent of the counterfeit medicines seized by the European Union Customs came from the United States.[544] In 2007, 1.04 percent of counterfeit foodstuff and beverages, 4.41 percent of counterfeit computer equipment, 2.39 percent of counterfeit toys and games, and 0.30 percent of counterfeit medicines seized by the European Union Customs officials were shipped from the United States.[545] Again, it is unknown whether these goods were manufactured in the United States or merely transshipped through the United States.

2. The magnitude of the threat

As stated earlier in this report, it is impossible to measure precisely the magnitude of the threat to United States interests from infringing goods from any country, even the United States. The OECD report did not separately estimate the amount of infringing goods coming into the United States. A very rough method for estimating this figure is to apply the estimated percentage of infringing goods overall to the amount of goods imported into the United States. The total value of imports of goods into the United States in 2010 was a little over $1.935 trillion. If one applied the OECD estimate that on average 1.95 percent of trade is counterfeit, then approximately $37 billion worth of physical infringing goods came into the United States in 2010.[**]

[*] There were a total of 26 cases. The report did not indicate how many of the cases were based on goods from the United States. In other words, it is unknown whether the nearly 50,000 goods were seized at one time or if there were multiple seizures. It should be noted that, unlike CBP which measures by number of seizures, the European Union measures by number of items.

[**] If the ICC/WCO estimates five to seven percent of imported goods are infringing, then the amount increases to between $96.75 and $135.45 billion in counterfeit goods attempting to enter the United States. Regardless of the multiplier that is used, these estimates do not include domestically produced and consumed physical counterfeit goods or online piracy. These figures should not be used to measure the percentage of infringing goods CBP and ICE seize annually as the value figures CBP and ICE use do not correspond to the OECD value figures.

Using a more sophisticated approach, the BASCAP report concluded in 2008 the United States consumed between $66 and $100 billion in infringing goods. Of this amount an estimated $45 to $60 billion came from outside the United States. Between $12 and $14 billion were estimated to have been domestically produced and consumed. Lastly, $9 to $25 billion of these figures were attributed to digitally pirated goods – including $7 to $20 billion from digitally pirated music, $1.2 to $2 billion from digitally pirated movies, and $64 million to $3 billion from digitally pirated software.[546] It is not possible to evaluate the reliability of these figures because of the lack of data supporting the assumptions upon which the figures are calculated.[*]

In addition to measuring the overall value of infringing goods produced and consumed in the United States, there are lost sales to industries from piracy and infringing goods consumed in the United States market. The only industries with significant research into loss figures from infringing goods in the United States are the music, film, and business software industries.

The music industry estimates 63 percent of music obtained in the United States is pirated.[547] This results in an estimated annual loss of approximately $151 million from physical piracy (eight percent of global physical piracy) and $890 million from digital piracy (two percent of global digital piracy).[548]

The Motion Picture Association (MPA) estimated the United States motion picture industry lost nearly $6.1 billion in 2005 from worldwide piracy. Approximately $864 million was from physical piracy in the United States (23 percent of global physical piracy), such as counterfeit DVDs, and $447 million was lost from digital piracy in the United States (19 percent of global digital piracy).[549]

The business software industry estimates that although the business software piracy rate in the United States of 20 percent is comparatively lower than most countries, the value of the domestically pirated software is approximately $8.4 billion. This is the single highest country value amount, even higher than the estimated value of piracy in China. This high figure is due to the higher penetration of computers in the United States as well as the pirating of more expensive software.

These figures indicate that although the United States has comparatively low levels of piracy, the economic losses from piracy in the United States are significant. Several factors account for the disparity between piracy levels and losses. The level of losses depends on the substitution rate applied. Removal of pirated options in countries such as China and India is not likely to significantly increase purchases of legitimate copies because these countries do not have substantial legitimate markets for American music, movies, and software. For example, China limits the number of foreign films that can be legitimately distributed each year in China to 20. Thus, many of the consumers of pirated movies in China do not have a legitimate alternative so the movie companies are not losing as much money as if there were a legitimate outlet for their movies.

[*] Notably BASCAP's own figures are inconsistent within its report. The total value of U.S. consumption is listed as $66 to $100 billion in the summary portion of the report but inexplicably in the text of the report the figures total $67 to $97 billion.

3. Offenders

As described in Section VI of this report, all types of offenders are known to engage in IPR violations in the United States.

4. Addressing the problem

The United States government and industry are actively collaborating to address the increasing prevalence of IP theft. For example, in December 2010 the IPEC announced a group of private companies* will form a new nonprofit organization to help deter illegal online pharmacies.[550] Increased criminal penalties are under consideration for IPR violations that threaten the public's health and safety. The Department of Justice has committed to funding public awareness campaigns to better educate the public about the potential risks from IP theft.[551] There have been increased collaboration and enforcement efforts between the various law enforcement agencies with IPR responsibilities, such as Operation In Our Sites version 2.0, Pangea, and Operation Network Raider.[552]

Despite significant steps to improve the enforcement of IPR violations, the United States faces several challenges to combat this threat effectively. For example, numerous databases exist to catalogue IPR violations and support IPR investigations. However, some of these databases are owned and maintained by private industry and are not available to law enforcement. Others are exclusive to law enforcement, preventing industry representatives from being able to take advantage of this information. No database is all-inclusive, even within industry specific databases.

Although the creation of the new nonprofit to address counterfeit pharmaceuticals is a significant achievement, numerous government and industry representatives expressed concerns regarding purchases of infringing goods via the Internet. Some legitimate companies, such as ISPs or online payment providers, appear to have been complicit in allowing IPR violations to occur using their services.[553] Improved regulation of the activity on legitimate companies' websites and subsequent referrals to and cooperation with law enforcement regulations can help lessen the significant IPR violations occurring online.

Numerous industry representatives opined the need for thorough yet swift criminal investigations to deter other individuals from committing IPR violations.[554] The United States has modified its criminal IP laws to address the changing nature of the IP threat and law enforcement has increased its efforts substantially over the last decade. Nevertheless, the criminals still view IPR violations as a low risk, high profit crime compared to other crimes. In addition, public perception is still that IP crime is victimless. Improved cooperation is needed between industry representatives, law enforcement agencies, prosecutors, and judges to help educate individuals at all levels of IPR enforcement about the nature of the IPR threat and the need for stricter penalties to help insure the public's safety.[555]

* American Express, eNom, GoDaddy, Google, MasterCard, Microsoft, PayPal, Neustar, Visa, and Yahoo!.

VIII. CONCLUSION

This report has shown the consequences of IP theft are not limited to rights holders whose IP is stolen, but include threats to the public's health and safety, national security and the safety of United States war fighters, the United States government from lost tax and customs revenue and misplaced jobs, and critical United States infrastructure. The threat from infringing goods originating from offenders in foreign countries is significant and shows no sign of abating. Although offenders in other countries are responsible for producing the majority of the infringing goods, the threat is furthered by offenders acting within the United States.

The threat continues to evolve. The trend toward producing goods for the primary market where consumers are deceived into believing they are purchasing genuine goods has increased the potential health and safety costs from counterfeit goods. The ability of criminals to circumvent or infiltrate the protections in legitimate supply chains will further confuse or deceive consumers. Finally, the increasing use of the Internet for commerce will only magnify the negative impact of this phenomenon.

Production and distribution of infringing goods provide a steady and significant revenue source for a broad array of offenders. As long as there are buyers of infringing goods, there are people who will provide them. The low risk from committing such crimes and the high profits reaped will continue to attract criminals and criminal organizations. Without improvement in identification, protection, and enforcement, these crimes and their negative impact will increase for the foreseeable future.

This multi-dimensional threat requires a multi-dimensional response. No industry or country is immune from the threat, nor can they address the threat alone. As Attorney General Eric Holder has noted, "stealing innovative ideas or passing off counterfeits can have devastating consequences for individuals, families, and communities. . . . Intellectual property crimes are not victimless. And we must make certain they are no longer perceived as risk-free." Armed with this improved understanding of the current threat to United States interests from IP theft, the United States government can improve its policy and enforcement efforts.

National Intellectual Property Rights Coordination Center Survey

Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of this product. Thank you for your cooperation and assistance.

Return to:
National Intellectual Property Rights Coordination Center
2451 Crystal Drive
STOP 5105
Arlington, VA 20598-5105

1. My employment can best be described as:
    a. Rights Holder/Industry Representative
    b. Law Enforcement Officer (including Federal)
    c. Government Employee
    d. Academia/Student
    e. Other: _____
2. My job assignment can best be described as:
    a. Legal
    b. Policy
    c. Diplomacy
    d. Investigative
    e. Research
    f. Other: _____
3. I primarily work in:
    a. the United States
    b. Asia
    c. Europe
    d. Africa
    e. North America, other than the United States
    f. South America
    g. Other: _____
4. My overall knowledge of IPR crime prior to reading this report was:
    a. Expert
    b. Advanced
    c. Intermediate
    d. Novice
    e. None
5. This report provided an informative overview of all aspects of IPR crime:
    a. Strongly Agree
    b. Somewhat Agree
    c. Neither Agree nor Disagree
    d. Somewhat Disagree
    e. Strongly Disagree

6. This report increased my knowledge regarding IPR crime:
    a. Strongly Agree
    b. Somewhat Agree
    c. Neither Agree nor Disagree
    d. Somewhat Disagree
    e. Strongly Disagree
7. Information presented in the report is consistent with my personal experiences/knowledge regarding IPR crime:
    a. Strongly Agree
    b. Somewhat Agree
    c. Neither Agree nor Disagree
    d. Somewhat Disagree
    e. Strongly Disagree
8. This report will be a useful reference tool for me/my employer:
    a. Strongly Agree
    b. Somewhat Agree
    c. Neither Agree nor Disagree
    d. Somewhat Disagree
    e. Strongly Disagree
9. This report was easy to understand:
    a. Strongly Agree
    b. Somewhat Agree
    c. Neither Agree nor Disagree
    d. Somewhat Disagree
    e. Strongly Disagree
10. The most helpful/informative/interesting information in this report was regarding:

    _____

    _____
11. I would like to have seen more information regarding:

    _____

    _____
12. Overall, I rate this report as:
    a. Excellent
    b. Good
    c. Average
    d. Fair
    e. Poor
13. Any additional comments:

    _____

    _____

For additional follow up regarding your survey, please include your contact information below (optional):

1. First and Last Name: _____
2. Employer/Organization: _____
3. Phone Number: _____
4. Email Address: _____

ENDNOTES

[1] The Prioritizing Resources and Organization for Intellectual Property Act of 2008, Title III, § 303 (e) (5), P.L 110-403.
[2] Executive Office of the President of the United States, Intellectual Property Enforcement Coordinator (IPEC), "2010 Joint Strategic Plan on Intellectual Property Enforcement," June 2010, 30, http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf (accessed 18 Apr. 2011).
[3] United States Department of Justice (DOJ), *Prosecuting Intellectual Property Crimes*, *3rd ed.*, Sept. 2006 (Washington DC: DOJ), 114-121.
[4] Office of the United States Intellectual Property Enforcement Coordinator, "Intellectual Property Spotlight," Aug. 2010, 2, http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/IPEC_Spotlight_August2010.pdf (accessed 18 Apr. 2011).
[5] Victoria Espinel, IPEC, Testimony Before the Subcommittee on Intellectual Property, Competition, and the Internet, Committee on the Judiciary, United State House of Representatives, 1 Mar. 2011, http://www.judiciary.house.gov/hearings/pdf/espinel03012011.pdf (accessed 18 Apr. 2011).
[6] Carlos M. Gutierrez, Secretary of U.S. Department of Commerce, "Get Moving on Patent Reform Measure Stalled in Senate," 11 May 2008, http://2001-2009.commerce.gov/NewsRoom/PressReleases_FactSheets/PROD01_005990 (accessed 18 Apr. 2011).
[7] Organisation for Economic Co-Operation and Development (OECD), "The Economic Impact of Counterfeiting and Piracy," 2008, 69, http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/OECD-FullReport.pdf (accessed 18 Apr. 2011) (2008 Report).
[8] Industry interview.
[9] OECD, "2008 Report," 305-306.
[10] Government interview.
[11] Government interviews.
[12] See, e.g., http://en.wikipedia.org/wiki/shanzai, (accessed 5 May 2011).
[13] Industry interview.
[14] Industry interview.
[15] David Lague, "Next Step for Counterfeiters: Faking the Whole Company," *The New York Times*, 1 May 2006, http://www.nytimes.com/2006/05/01/technology/01pirate.html? (accessed 18 Apr. 2011).
[16] OECD, "2008 Report," 84.
[17] Industry interviews.
[18] Industry interview.
[19] Brian Grow, Chi-Chu Tschang, Cliff Edwards, and Brian Burnsed, "Dangerous Fakes," *Businessweek*, 2 Oct. 2008, http://www.businessweek.com/magazine/content/08_41/b4103034193886.htm (accessed 11 Jan. 2011).
[20] Grow, et al., "Dangerous Fakes," *Businessweek*.
[21] Industry interviews.
[22] DOJ, "1136 Defenses," *Criminal Resource Manual*, *United States Attorney's Manual*, *Title 9*, updated Oct. 2004, http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm01136.htm (accessed 22 Feb. 2011).
[23] Industry interview.
[24] Motion Picture Association of America (MPAA), "Types of Content Theft," 2010, http://www.mpaa.org/contentprotection/types-of-content-theft (accessed 15 Feb. 2011).
[25] Industry interview.
[26] Symantec Corp., "More Than Half of Ex-Employees Admit to Stealing Company Data According to New Study," *Press Release*, 23 Feb. 2009, http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01 (accessed 12 May 2011).
[27] DOJ, "Chinese National Pleads Guilty to Stealing Ford Trade Secrets," *Press Release*, 17 Nov. 2010, http://www.justice.gov/criminal/cybercrime/yuPlea.pdf (accessed 5 Jan. 2011).
[28] DOJ, "Former Intel Employee Indicted for Stealing more than $1 Billion of Trade Secrets," *Press Release*, 5 Nov. 2008, http://www.justice.gov/criminal/cybercrime/paniIndict.pdf (accessed 5 Jan. 2011).
[29] Investigative information.
[30] Government interviews.
[31] Industry interview; Government interview.

[32] Industry interview.
[33] Industry interview.
[34] See, e.g., OECD, "2008 Report," 86; Government interview.
[35] OECD, "2008 Report," 85-86.
[36] Motor & Equipment Manufacturers Association (MEMA) Brand Protection Council, "Understanding the Flow of Counterfeit and Gray Market Goods though the U.S. Automotive and Commercial Vehicle Parts Marketplace," Jan. 2009, 6, http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Understanding%20the%20Flow%20of%20Counterfeit%20and%20Gray%20Market%20Goods%20though%20the%20U.S.%20Automotive%20and%20Commercial%20Vehicle%20Parts%20Marketplace.pdf (accessed 18 Apr. 2011).
[37] Industry interview.
[38] Government interview.
[39] DOJ, "Progress Report of the Department of Justice's Task Force on Intellectual Property," June 2006, 26, http://www.justice.gov/criminal/cybercrime/2006/IPTFProgressReports(6-19-06).pdf (accessed 9 Feb. 2011).
[40] Doug Palmer and Melanie Lee, "Special Report: Faked in China: Inside the Pirates' Web," *Reuters*, 26 Oct. 2010, http://www.reuters.com/article/2010/10/26/us-china-counterfeit-idUSTRE69P1AR20101026 (accessed 20 Feb. 2011).
[41] Grow, et al., "Dangerous Fakes," *Businessweek*.
[42] Industry interviews.
[43] Industry interview.
[44] For similar examples in other industries see, U.S. Department of Commerce, Office of Technology Evaluation "Defense Industrial Base Assessment: Counterfeit Electronics," Jan. 2010, 30, http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf, (accessed 18 Apr. 2011) (Defense Industrial Base).
[45] Industry interview.
[46] See generally OECD, "2008 Report;" see also generally OECD, "Magnitude of Counterfeiting and Piracy of Tangible Products: An Update," Nov. 2009, http://www.oecd.org/dataoecd/57/27/44088872.pdf (accessed 18 Apr. 2011) (2009 Update).
[47] OECD, "2009 Update," 1. For a more thorough discussion of the relative merits and difficulties regarding quantifying the economic effects of infringing goods see Government Accountability Office (GAO), "Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods, " GAO-10-423, 12 Apr. 2010.
[48] OECD, "2008 Report," 71.
[49] Frontier Economics, "Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report Commissioned by the Business Action to Stop Counterfeiting and Piracy (BASCAP)," Feb. 2011, 5 (Estimating Global Impact).
[50] Frontier Economics, "Estimating Global Impact," 4.
[51] Frontier Economics, "Estimating Global Impact," 6.
[52] Frontier Economics, "Estimating Global Impact," 8.
[53] Frontier Economics, "Estimating Global Impact," 5.
[54] International AntiCounterfeiting Coalition (IACC), "The Negative Consequences of International Intellectual Property Theft: Economic Harm, Threats to the Public Health and Safety, and Links to Organized Crime and Terrorist Organization, " Jan. 2005, 2 http://counterfeiting.unicri.it/docs/International%20AntiCounterfeiting%20Coalition.White%20Paper.pdf (accessed 2 May 2011) (IACC, Negative Consequences).
[55] GAO, "Better Data Analysis and Integration Could Help U.S. Customs and Border Protection Improve Border Enforcement Efforts," GAO-07-735, 26 Apr. 2007, 4.
[56] United States Customs and Border Protection (CBP) and United States Immigration and Customs Enforcement (ICE), "Intellectual Property Rights Fiscal Year 2010 Seizure Statistics – Final Report," Jan. 2011, 4.
[57] European Commission – Taxation and Customs Union, "Report on EU Customs Enforcement of Intellectual Property Rights: Results at the EU Border – 2009," 9, http://ec.europa.eu/taxation_customs/resources/documents/customs/customs_controls/counterfeit_piracy/statistics/statistics_2009.pdf (accessed 2 May 2011).
[58] Frontier Economics, "Estimating Global Impact," 16.
[59] OECD, "2008 Report," 70.

[60] IACC, "Negative Consequences," 2.
[61] IACC, "Negative Consequences," 2-3.
[62] ICC Counterfeiting Intelligence Bureau, "The International Anti-Counterfeiting Directory," 28.
[63] World Customs Organization, "Enforcement and Compliance – Responsibilities > The WCO and the protection of Intellectual Property Rights," http://www.wcoomd.org/valelearningoncustomsvaluation_epipr.htm (accessed 15 Feb. 2011).
[64] Internet World Stats, "Internet Usage Statistics – The Internet Big Picture, Internet Users and Population Stats," 30 Apr. 2011, http://www.internetworldstats.com/stats.htm (accessed 15 Feb. 2011) (Internet Big Picture).
[65] Internet World Stats, "Internet Big Picture," Internet World Stats, "China Internet Usage Stats and Population Report," 30 Mar. 2011, http://www.internetworldstats.com/asia/cn.htm (accessed 15 Feb. 2011).
[66] International Telecommunications Union (ITU), "The World in 2010: ICT Facts & Figures," 19 Oct. 2010, slide 6, http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf (accessed 18 Apr. 2011).
[67] Nielsen, "Trends in Online Shopping a global Nielsen consumer report," *Nielsen online*, Feb. 2008, 1, http://id.nielsen.com/news/documents/GlobalOnlineShoppingReportFeb08.pdf (accessed 18 Apr. 2011).
[68] Frontier Economics, "The Impact of Counterfeiting on Governments and Consumers," May 2009, 8, http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Impact%20of%20Counterfeiting%20on%20Governments%20and%20Consumers%20-%20Exec%20Summary.pdf, (accessed 18 Apr. 2011) (Impact of Counterfeiting).
[69] Frontier Economics, "Impact of Counterfeiting," 8, 23-24.
[70] Frontier Economics, "Impact of Counterfeiting," 6.
[71] Frontier Economics, "Impact of Counterfeiting," 6.
[72] Stephen E. Siwek, Institute for Policy Innovation, IPI Center for Technology Freedom, "The True Cost of Sound Recording Piracy to the U.S. Economy," *Policy Report 188*, Aug. 2007, 5-6.
[73] Motion Picture Association (MPA) and L.E.K., "The Cost of Movie Piracy," 2008, 4, http://mpa-i.org/pdf/leksummaryMPA%20revised1.2008.pdf, (accessed 18 Apr. 2011).
[74] Frontier Economics, "Impact of Counterfeiting," 9.
[75] Elizabeth Lux, "Brand Value," *The Wall Street Journal*, 6 Oct. 2010, http://online.wsj.com/article/SB10001424052748704206804575467690964993952.html (accessed 13 May 2011).
[76] Lux, "Brand Value."
[77] Interbrand Study Results, "Best Global Brands 2010 Rankings," http://www.interbrand.com/en/knowledge/best-global-brands/best-global-brands-2008/best-global-brands-2010.aspx (accessed 18 Apr. 2011).
[78] Lux, "Brand Value."
[79] United Nations Office on Drugs and Crime (UNODC), "The Globalization of Crime: A Transnational Organized Crime Threat Assessment," 17 June 2010, 36, http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf (accessed 12 May 2011) (Globalization of Crime).
[80] BBC News, "Business: The Company File, Belgium bans Coca Cola," *BBC News Online*, 14 June 1999 http://news.bbc.co.uk/2/hi/europe/369089.stm, (accessed 18 Feb. 2011).
[81] Interbrand, "Best Global Brands."
[82] Industry interview.
[83] Frontier Economics, "Estimating Global Impact," 47.
[84] Frontier Economics, "Estimating Global Impact," 44.
[85] Frontier Economics, "Impact of Counterfeiting," 9.
[86] Frontier Economics, "Estimating Global Impact," 47.
[87] Frontier Economics, "Estimating Global Impact," 44.
[88] ICE, "'Safe Summer' operations seize tons of potentially harmful counterfeit items in US and Mexico," *Press Release*, 5 Oct. 2010, http://www.ice.gov/news/releases/1010/101005washingtondc.htm (accessed 11 May 2011) (Safe Summer Operations); Executive Office of the President of the United States, "2010 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement," Feb. 2011, 21, http://www.ice.gov/doclib/iprcenter/pdf/ipec-annual-report.pdf (accessed 11 May 2011) (2010 IPEC Annual Report).
[89] ICE, "'Safe Summer Operations," Executive Office of the President of the United States, "2010 IPEC Annual Report," 21.
[90] CBP and ICE, "Intellectual Property Rights Seizure Statistics: Fiscal Year 2009," Oct. 2009, 10; CBP and ICE, "Intellectual Property Rights Seizure Statistics: Fiscal Year 2008," Jan. 2009, 11.
[91] Government interview.

[92] Consumer Product Safety Commission (CPSC), "Scott Electric Co. Inc. Recalls Counterfeit Circuit Breakers Due to Fire Hazard," *Press Release #07-036*, 16 Nov. 2006, 1.
[93] Majid Yar, "A Deadly Faith in Fakes: Trademark Theft and the Global Trade in Counterfeit Automotive Components," *Internet Journal of Criminology*, 2005, 11-13, http://www.internetjournalofcriminology.com/Yar%20-%20A%20Deadly%20Faith%20in%20Fakes.pdf, (accessed 18 Apr. 2011).
[94] World Customs Organization, "The first review: Customs and Counterfeiting 2004," *Press Release*, 18 Aug. 2006, http://www.wcoomd.org/press/?v=1&lid=1&cid=1&id=125, (accessed 18 Apr. 2011).
[95] Frontier Economics, "Estimating Global Impact," 1.
[96] Frontier Economics, "Estimating Global Impact," 7 (referencing Frontier Economics, "Impact of Counterfeiting").
[97] U.S. Department of Commerce, "Defense Industrial Base," 30.
[98] U.S. Department of Commerce, "Defense Industrial Base," 178.
[99] DOJ, "Owner and Employee of Florida-based Company Indicted in Connection with Sales of Counterfeit High Tech Devices Destined to the U.S. Military and Other Industries," *Press Release*, 14 Sept. 2010, 2, http://www.justice.gov/criminal/cybercrime/wrenIndict.pdf (accessed 18 Apr. 2011) (Counterfeit High Tech Devices).
[100] Government interviews.
[101] Industry interview.
[102] National Aeronautics and Space Administration (NASA), "The Counterfeiting Epidemic: How to Avoid Fake Parts," 9-10 Feb. 2010, 15 (quoting the American Electronic Resource, Inc.).
[103] NASA, "The Counterfeiting Epidemic: How to Avoid Fake Parts," presentation NASA PM Challenge, 9-10 Feb. 2010, 21.
[104] Government interview.
[105] Grow, et al., "Dangerous Fakes."
[106] DOJ, "Counterfeit High Tech Devices," 1.
[107] DOJ, "California Operations Manager for MBP Micro, Inc. Pleads Guilty in Connection with Sales of Counterfeit High Tech Parts to the U.S. Military," *Press Release*, 20 Nov. 2009, 1, http://www.justice.gov/criminal/cybercrime/felahyPlea.pdf (accessed 15 Feb. 2011).
[108] DOJ, "Departments of Justice and Homeland Security Announce 30 Convictions, More than $143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware," *Press Release*, 6 May 2010, http://www.justice.gov/criminal/cybercrime/ashoorConvict.pdf (accessed 26 Apr. 2011) (Counterfeit Network Hardware).
[109] FBI, "Pirated Software: A Potential Intelligence-Gathering Tool Leaves US Government, Businesses, and Persons Vulnerable to Compromise," *Threat Assessment*, 21 June 2010, 9 (Pirated Software).
[110] Grow, et al., "Dangerous Fakes."
[111] FBI, "Pirated Software," 6.
[112] U.S.-China Economic and Security Review Commission (China Commission), "2008 Report to Congress," Nov. 2008, 166-67, http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf (accessed 13 May 2011); Brian Grow, "The Threat Posed by Fake Cisco Parts," *Businessweek*, 2 Oct. 2008, www.businessweek.com/print/magazine/content/08_41/b4103038201037.htm (accessed 13 May 2011).
[113] U.S. Department of Commerce, "Defense Industrial Base," 16.
[114] Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," (Congressional Research Service, 15 Nov. 2007), 15, http://assets.opencrs.com/rpts/RL32114_20071115.pdf.
[115] DOJ, "Counterfeit Network Hardware."
[116] FBI, "Theft of Trade Secrets 2009," 4.
[117] Siwek, "The True Cost of Sound Recording Piracy to the U.S. Economy," 5.
[118] Industry interview.
[119] Frontier Economics, "Estimating Global Impact," 25.
[120] Recording Industry Association of America, "The Volume of Music Acquired Without Payment," *Let's Play,* 2010, 11.
[121] Industry interview.
[122] International Federation of the Phonographic Industry (IFPI), "IFPI Digital Music Report 2011," 2011, 21, http://www.ifpi.org/content/library/DMR2011.pdf (accessed 13 May 2011) (Digital Music Report 2011).
[123] Industry interview.
[124] Industry interview.

[125] Industry interview.
[126] MPA and L.E.K., "The Cost of Movie Piracy," 4.
[127] MPAA, *Theatrical Market Statistics*, 2010, 3; Alex Dobuzinskis, "Film box office overtakes DVD, Blu-ray sales," *Reuters*, *4* Jan. 2010, http://www.reuters.com/assets/print?aid=USN0422438220100105 (accessed 25 Apr. 2011).
[128] IFPI, "Digital Music Report 2011," 23.
[129] Ronald Grover, "Hollywood is Worried as DVD Sales Slow," *Businessweek*, 19 Feb. 2009, http://www.businessweek.com/print/magazine/content/09_09/b4121056770437.htm (accessed 25 Apr. 2011).
[130] MPA and L.E.K., "The Cost of Movie Piracy," 4.
[131] IFPI, "Digital Music Report 2011," 23; Industry interview.
[132] "Avatar Crowned the Most Pirated Movie of 2010," 20 Dec. 2010, http://torrentfreak.com/avatar-crowned-the-most-pirated-movie-of-2010-101220/ (accessed 5 May 2011).
[133] Industry interview.
[134] International Intellectual Property Association (IIPA), "IIPA's 2010 Special 301 Report," Counsel Letter to Stan McCoy, Assistant United States Trade Representative, 15 Feb. 2011, 9, http://images.bluzone2087.multiply.multiplycontent.com/attachment/0/S5dA5wooCoAAAAaqK8M1/USTR-2010-0003-0287.1.pdf?nmid=322834520 (accessed 2 May 2011) (2010 Special 301 Report Letter).
[135] Industry interview.
[136] Business Software Alliance (BSA), "Seventh Annual BSA-IDC Global Software 09 Piracy Study," May 2010, Executive Summary (09 Piracy Study).
[137] BSA, "09 Piracy Study," Executive Summary.
[138] BSA, "09 Piracy Study," Executive Summary.
[139] IIPA, "2010 Special 301 Report Letter."
[140] Industry interview.
[141] FBI, "International Investigation Conducted Jointly by FBI and Law Enforcement Authorities in People's Republic of China Results in Multiple Arrests in China and Seizures of Counterfeit Microsoft and Symantec Software," 23 July 2007, www.justice.gov/criminal/cybercrime/summerArrest.htm (accessed 25 Apr. 2011).
[142] Industry interview.
[143] BSA, "Software Piracy on the Internet: A Threat to Your Security," Oct. 2009, http://portal.bsa.org/internetreport2009/2009internetpiracyreport.pdf, 13.
[144] BSA, "09 Piracy Study," Executive Summary.
[145] BSA, "09 Piracy Study," Executive Summary.
[146] MarkMonitor, "Traffic Report: Online Piracy and Counterfeiting," January 2011, 4.
[147] IFPI, "Digital Music Report 2010," 2010, 18, http://www.ifpi.org/content/library/DMR2010.pdf (accessed 13 May 2011).
[148] Siwek, "The True Cost of Sound Recording Piracy to the U.S. Economy;" Stephen E. Siwek, Institute for Policy Innovation, IPI Center for Technology Freedom, "The True Cost of Motion Picture Piracy to the U.S. Economy," *Policy Report 186*, Sept. 2006.
[149] China Commission, "2008 Report to Congress," 167; Brian Grow, Keith Epstein, Chi-Chu Tschang, "The New E-spionage Threat," *Businessweek*, 10 Apr. 2008, www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm (accessed 13 May 2011); Grow, "The Threat Posed by Fake Cisco Parts."
[150] BSA, "Software Piracy on the Internet: A Threat to Your Security," Oct. 2009, http://portal.bsa.org/internetreport2009/ (accessed 13 May 2011); Brian Krebs and Ellen Nakashima, "File Sharing Leaks Sensitive Federal Data, Lawmakers Are Told," *The Washington Post,"* 30 July 2009; FBI, "Pirated Software," 4.
[151] BSA, "Online Software Scams: A Threat to Your Security," Oct. 2008, http://www.bsa.org/files/Internet_Piracy_Report.pdf (accessed 25 Apr. 2011); FBI, "Pirated Software," 8; Krebs and Nakashima, "File Sharing Leaks Sensitive Federal Data."
[152] Molly McHugh, "Pirated Microsoft software funded Mexican drug cartel," *Digital Trends*, 4 Feb. 2011, 1.
[153] Randall W. Lutter, Acting Associate Commissioner for Policy and Planning, Food and Drug Administration, "Counterfeit Drugs," Statement before the Subcommittee on Criminal Justice, Drug Policy, and Human Resources, House Committee on Oversight Government Reform, 1 Nov. 2005, http://www.fda.gov/NewsEvents/Testimony/ucm112670.htm (accessed 11 May 2011).

[154] Roger Bate, "Fake Drugs: Causes, Consequences, and Possible Solutions," *American Enterprise Institute for Public Policy Research*, 3 Mar. 2010, http://www.aei.org/speech/100125 (accessed 25 Apr. 2011).
[155] Randall W. Lutter, Associate Commissioner for Policy and Planning, Food and Drug Administration, "Pharmaceutical Supply Chain Security," Statement before the Subcommittee on Criminal Justice, Drug Policy, and Human Resources, House Committee on Oversight Government Reform, 11 July 2006, http://www.fda.gov/NewsEvents/Testimony/ucm111440.htm (accessed 11 May 2011).
[156] World Health Organization, "Substandard and Counterfeit Medicines," *Fact Sheet No 275*, Nov. 2003, http://www.who.int/mediacentre/factsheets/2003/fs275/en/ (accessed 13 May 2011).
[157] "Poison Pills," *The Economist*, 2 Sept. 2010, http://www.economist.com/node/16943895 (accessed 3 May 2011).
[158] Charles Corey, "Counterfeit Drugs Pose Dangers in 90 Countries Worldwide," Embassy of the United States of America, Brussels, Belgium, 14 Oct. 2010, http://www.uspolicy.be/headline/counterfeit-drugs-pose-dangers-90-countries-worldwide (accessed 25 Apr. 2011).
[159] ICC Counterfeiting Intelligence Bureau (CIB), "The International Anti-Counterfeiting Directory 2009," 25.
[160] Interpol, "Operation Pangea III – International Internet Week of Action – Final Report," 5-12 Oct. 2010.
[161] ICC CIB, "The International Anti-Counterfeiting Directory 2009," 25.
[162] "Poison Pills."
[163] ICC CIB, "The International Anti-Counterfeiting Directory 2009," 25.
[164] ICC CIB, "The International Anti-Counterfeiting Directory 2009," 25.
[165] Kathy Chu, "Growing problem of fake drugs hurting patients, companies," *USA Today*, 13 Sept. 2010, http://www.usatoday.com/money/industries/health/2010-09-12-asia-counterfeit-drugs_N.htm (accessed 25 Apr. 2011).
[166] World Health Organization (WHO), "Medicines: Counterfeit Medicines," Fact Sheet No. 275, January 2010, http://www.who.int/mediacentre/factsheets/fs275/en/ (accessed 27 Apr. 2011).
[167] Industry interviews.
[168] WHO, "Medicines: Counterfeit Medicines."
[169] WHO, "Medicines: Facts and Figures," http://www.euro.who.int/en/what-we-do/health-topics/Health-systems/medicines/country-work (accessed 13 May 2011).
[170] Charles Clift, "Counterfeit Medicines: Health and Harm," *The World Today*, Vol. 66.12, Dec. 2010, 12, http://www.chathamhouse.org.uk/publications/twt/archive/view/-/id/2102/ (accessed 27 Apr. 2011).
[171] Pew Prescription Project, "Americans' Attitudes on Prescription Drug Safety," Apr. 2010, 3, http://www.prescriptionproject.org/tools/initiatives_resources/files/Drug-Safety-Poll-Findings-2.pdf (accessed 5 May 2011).
[172] Pew Prescription Project, "Americans' Attitudes on Prescription Drug Safety," 7.
[173] ICC CIB, "The International Anti-Counterfeiting Directory 2009," 25.
[174] ICC CIB, "The International Anti-Counterfeiting Directory 2009," 25.
[175] Charles Corey, "Counterfeit Drugs Pose Dangers in 90 Countries Worldwide" (quoting Rubie Mages, director of strategic planning for global security at Pfizer).
[176] ICC Counterfeiting Intelligence Bureau, "The International Anti-Counterfeiting Directory 2009," 25.
[177] Government Accountability Office (GAO), "Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts," *GAO Report GAO-10-3889*, Mar. 2010, 4 (Defense Supplier Base).
[178] U.S. Department of Commerce, "Defense Industrial Base," 150.
[179] Government interview.
[180] U.S. Department of Commerce, "Defense Industrial Base," 178.
[181] U.S. Department of Commerce, "Defense Industrial Base," 6.
[182] Government interviews; Government statistics sheet.
[183] GAO, "Defense Supplier Base," 11.
[184] DOJ, "Counterfeit Network Hardware."
[185] NASA, "The Counterfeiting Epidemic: How to Avoid Fake Parts," 15.
[186] DOJ, "Selling Counterfeit Cisco Parts To Bureau Of Prisons Means Owner Of Syren Technology Will Now Spend Time There," *Press Release*, 7 Sept. 2010, http://www.justice.gov/criminal/cybercrime/edmanSent.pdf ; see also, Glenn Derene And Joe Pappalardo, Counterfeit Chips Raise Big Hacking, Terror Threats, Experts Say, 1 Oct. 2009, http://www.popularmechanics.com/technology/gadgets/news/4253628 (accessed 13 May 2011).
[187] ICE, "Initiative nets $143 million in Cisco goods," *ICE News Release*, 6 May 2010, 1. http://www.ice.gov/news/releases/1005/100506washingtondc.htm (accessed 27 Apr. 2011).

[188] Industry interview; Government interview.
[189] FBI, "Counterfeit Aircraft Parts and Illicit Networks: A National Threat Assessment," *Intelligence Assessment*, 9 July 2010, 10 (Counterfeit Aircraft Parts).
[190] FBI, "Counterfeit Aircraft Parts," 10.
[191] Government interview.
[192] "An Unnerving Reality," *Aerospace Manufacturing and Design*, 4 Feb. 2009, http://www.onlineamd.com/Article.aspx?article_id=63448 (accessed 27 Apr. 2011).
[193] Aerospace Industries Association, "Counterfeit Parts: Increasing Awareness and Developing Countermeasures," Mar. 2011, 13.
[194] FBI, "Counterfeit Aircraft Parts," 8.
[195] FBI, "Counterfeit Aircraft Parts," 5.
[196] FBI, "Counterfeit Aircraft Parts," 10.
[197] Government interview.
[198] Government interviews.
[199] J. Reed, "Fake Parts Are Seeping Into Military Aircraft Maintenance Depots," *Inside the Air Force*, Vol. 19.13, 28 Mar. 2008, 1, http://www.verical.com/about/resources/docs/032808_AirForce_FAKE_PARTS_ARE_SEEPING_INTO_MILITARY_AIRCRAFT_MAINTENANCE_DEPOTS.pdf (accessed 13 May 2011).
[200] U.S. Chamber of Commerce, Global Intellectual Property Center, "New Balance," *Intellectual Property Protection and Enforcement Manual*, 41, http://www.ipr-policy.eu/media/pts/1/Brand_Enforcement_Manual_FINAL.pdf (accessed 13 May 2011).
[201] Industry interview.
[202] UNODC, "Globalization of Crime," 173.
[203] CBP and ICE, "Intellectual Property Rights Fiscal Year 2010 Seizure Statistics – Final Report," 13.
[204] Industry interview.
[205] Industry interview.
[206] See, e.g., Victoria Espinel, Intellectual Property Enforcement Coordinator (IPEC), "Protecting U.S. Intellectual Property Overseas: The Joint Strategic Plan and Beyond," Testimony at the Hearing before the Committee on Foreign Affairs, House of Representatives, One Hundred Eleventh Congress, Second Session," 21 July 2010, Serial 111-111, 25-26, http://foreignaffairs.house.gov/111/57607.pdf (accessed 4 May 2011).
[207] DOJ, "Norwood Man Pleads Guilty to Selling Counterfeit Clothing and Accessories," *Press Release*, 23 Feb. 2000, http://www.justice.gov/criminal/cybercrime/kablin.htm (accessed 3 May 2011).
[208] United Nations Interregional Crime and Justice Research Institute (UNICRI), "Counterfeiting: A Global Spread, a Global Threat," 110, http://counterfeiting.unicri.it/report2008.php (accessed 27 Apr. 2011) (Counterfeiting: A Global Spread).
[209] National Intellectual Property Rights Coordination Center (IPR Center), "Intellectual Property Crime: Threats to the United States," 22 June 2010, 6 (IP Crime Threats).
[210] See, e.g., Ronald K. Noble, Secretary General of INTERPOL, "The links between intellectual property crime and terrorist financing," Text of public testimony before the United States House Committee on International Relations, One Hundred Eighth Congress, 16 July 2003, http://www.interpol.int/public/ICPO/speeches/SG20030716.asp?HM=1 (accessed 9 May 2011) ("the link between organized crime groups and counterfeit goods is well established"); see also UNICRI, "Counterfeiting: A Global Spread," 103 (links between counterfeiting and organized crime are "broadly acknowledged").
[211] See, e.g., UNICRI, "Counterfeiting: A Global Spread," 110-112.
[212] DOJ, "International Investigation Conducted Jointly By FBI and Law Enforcement Authorities in People's Republic Of China Results In Multiple Arrests In China And Seizures of Counterfeit Microsoft And Symantec Software," *Press Release*, 23 July 2007, http://www.justice.gov/criminal/cybercrime/summerArrest.htm (accessed 8 Feb. 2011) (Counterfeit Microsoft and Symantec Software).
[213] DOJ, "Federal Racketeering Indictments Target International Smuggling, Counterfeit Currency Operation," *Press Release*, 22 August 2005, http://www.atf.gov/press/releases/2005/08/082205-doj-multiple-racketeering-indictments.html (accessed 8 Feb. 2011).
[214] DOJ, "Counterfeit Microsoft And Symantec Software."
[215] Investigative information.

[216] United States Attorney Southern District of New York, "U.S. Indicts 51 Chinese Organized Crime Figures and Associates in Massive Coordinated Sweep," *Press Release,* 12 Nov. 2004, www.justice.gov/usao/nys/pressrelease/November04/chineseocindictment.pdf (accessed 7 Feb. 2011) (Chinese Organized Crime Figures).
[217] DOJ, "Progress Report of the Department of Justice's Task Force on Intellectual Property," June 2006, 26, www.justice.gov/criminal/cybercrime/2006IPTFProgressReports(6-19-06).pdf (accessed 9 Feb. 2011).
[218] DOJ, "U.S. Indicts 39 Members and Associates of a Major, Violent Criminal Organization," *Press Release*, 4-5, http://www.justice.gov/usao/nys/pressreleases/September05/pandaindictmentpr.pdf (accessed 3 May 2011).
[219] DOJ, "Progress Report of the Department of Justice's Task Force on Intellectual Property," 26; United States Attorney Southern District of New York, "Chinese Organized Crime Figures."
[220] Government interview.
[221] Government interview.
[222] Industry interview; Academia interview.
[223] Industry interviews.
[224] Investigative information.
[225] UNICRI, "Counterfeiting: A Global Spread, a Global Threat," 118.
[226] UNICRI, "Counterfeiting: A Global Spread, a Global Threat," 114; RAND Corporation, *Film Piracy, Organized Crime, and Terrorism,* 2009, http://www.rand.org/pubs/monographs/MG742.html (accessed 29 Apr. 2011) (Film Piracy).
[227] UNICRI, "Counterfeiting: A Global Spread," 110.
[228] DOJ, "Progress Report of the Department of Justice's Task Force on Intellectual Property," 26.
[229] United States Attorney Southern District of New York, "Chinese Organized Crime Figures."
[230] Industry interviews; Open Source Center, "Police Seize Pirated Goods from Zetas in Tabasco," *Highlights: Mexico Southeastern Crime/Narcotics/Security Issues 12 Mar 10*, 12 Mar. 2010, LAP20100312470001, https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_200_203_121123_43/content/Display/LAP20100312470001#index=1&searchKey=5095986&rpp=10 (accessed 29 Apr. 2011).
[231] Cass Ballenger, "Intellectual Property Crimes: Are Proceeds from Counterfeited Goods Funding Terrorism?" Testimony at House of Representatives, Hearing before the Committee on International Relations, One Hundred Eighth Congress, First Session, Serial 108-48, Washington, DC, 16 July 2003, 16, http://commdocs.house.gov/committees/intlrel/hfa88392.000/hfa88392_0f.htm (accessed 7 Feb. 2011) (Ballenger testimony); see also "Protecting U.S. Intellectual Property Overseas: The Joint Strategic Plan and Beyond, Hearing before the Committee on Foreign Affairs, House of Representatives, One Hundred Eleventh Congress, Second Session," (see specifically testimony of Mr. Deutch, "Intellectual property theft, as I raised earlier, has been increasingly funding to the terrorist organizations like Hamas and Hezbollah, an egregious example of which there are, frankly, too many to list, involves counterfeiters in tri-border area of South America who have provided millions of dollars in direct contributions to Hezbollah through their IP piracy. In fact, one such specially designated global terrorist entity in Paraguay provided the payment of millions of dollars directly to Hezbollah."); Rex Hudson, Library of Congress Federal Research Division, "Terrorist and Organized Crime Groups in the Tri-Border Area (TBA) of South America," July 2003 (revised Dec. 2010), http://www.loc.gov/rr/frd/pdf-files/TerrOrgCrime_TBA.pdf (accessed 22 Feb. 2011) (Terrorist and Organized Crime Groups in the TBA).
[232] Ballenger testimony, 16.
[233] RAND Corporation, *Film Piracy;* Hudson, "Terrorist and Organized Crime Groups in the TBA."
[234] Asa Hutchinson, Under Secretary for Border and Transportation Security, US Department of Homeland Security, "Intellectual Property Crimes: Are Proceeds from Counterfeited Goods Funding Terrorism?" Testimony at House of Representatives, Hearing before the Committee on International Relations, One Hundred Eighth Congress, First Session, Serial 108-48, Washington, DC, 16 July 2003, 42, http://commdocs.house.gov/committees/intlrel/hfa88392.000/hfa88392_0f.htm (accessed 7 Feb. 2011); Hudson, "Terrorist and Organized Crime Groups in the TBA."
[235] DOJ, "Progress Report of the Department of Justice's Task Force on Intellectual Property," 26.
[236] John T. Morton, Director of ICE, "Protecting U.S. Intellectual Property Overseas: The Joint Strategic Plan and Beyond," Testimony at Hearing before the Committee on Foreign Affairs, House of Representatives, One Hundred Eleventh Congress, Second Session," 21 July 2010, 54, http://foreignaffairs.house.gov/111/57607.pdf (accessed 13 May 2011).
[237] United States Department of the Treasury, "U.S. Designated Ibrahim as Terrorist Supporter," *Press Release*, 16 Oct. 2003, http://www.treasury.gov/press-center/press-releases/pages/js909.aspx (accessed 9 May 2011).

[238] United Nations Security Council, Department of Public Information, "Security Council Al-Qaida, Taliban Sanctions Committee Approves Changes to Consolidated List," 25 July 2006, http://www.un.org/News/Press/docs/2006/sc8785.doc.htm (accessed 21 Mar. 2011).
[239] IPR Center, "IP Crime Threats," 8.
[240] Joe Karaganis, Pedro Mizukami, Lawrence Liang, John Cross, and Olga Sezneva, ""Does Crime Pay? MPEE's Findings on Piracy, Organized crime, and Terrorism," 2011, 2, 12, http://piracy.ssrc.org/wp-content/uploads/2011/02/Does-Crime-Pay.pdf (accessed 13 May 2011).
[241] "Al-Qa'idah training in fake branded goods," *BBC Monitoring Reports*, 11 Sept. 2002.
[242] Ronald K. Noble, Secretary General of INTERPOL, "The Links Between Intellectual Property Crime and Terrorist Financing," Testimony before the United States House Committee on International Relations, One Hundred Eighth Congress, 16 July 2003, 23, http://commdocs.house.gov/committees/intlrel/hfa88392.000/hfa88392_0f.htm (accessed 13 May 2011) (6 July Testimony)..
[243] Noble, "The links between intellectual property crime and terrorist financing," Prepared statement for the United States House Committee on International Relations, One Hundred Eighth Congress, 16 July 2003, http://www.interpol.int/public/ICPO/speeches/SG20030716.asp?HM=1 (accessed 9 May 2011)
[244] See, e.g. Willy Stern, "Why Counterfeit Goods May Kill," *Businessweek*, 2 Sept. 1996, 6; Roslyn Mazer, "From T-Shirts to Terrorism," *The Washington Post*, 30 Sept. 2001, http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A43957-2001Sep29&notFound=true (accessed 12 Feb. 2011); John Solomon and Ted Bridis, "Feds Track Counterfeit Goods Sales," *Associated Press Online*, 24 Oct. 2002; James Nurton, "Why counterfeiting is not so harmless," *Managing Intellectual Property*, Sept. 2002, 43; Kathleen Millar, "Financing Terror: Profits from counterfeit goods pay for attacks," *U.S. Customs Today*, Nov. 2002, http://www.cbp.gov/xp/CustomsToday/2002/November/interpol.xml (accessed 12 Feb. 2011); IACC, "Negative Consequences," 20; Moisés Naím, *Illicit: How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy*, (Doubleday: New York 2005), 127.
[245] James Pettler, Federal Document Clearing House, "Trademark Counterfeiting," *FDCH Congressional Hearings Summaries*, 10 Oct. 1995, 2.
[246] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Executive Summary," 2004, http://www.9-11commission.gov/report/911Report_Exec.htm (accessed 3 May 2011).
[247] See generally, National Gang Intelligence Center (NGIC), "National Gang Threat Assessment 2009," Jan. 2009.
[248] NGIC, "National Gang Threat Assessment 2009," 3.
[249] Industry interview; Government interview.
[250] Industry interview.
[251] Investigative Consultants, "Florencia 13 and White Fence Gang Members Arrested," *IP Crimes*, Sept. 2010, 8.
[252] Government report.
[253] Industry interviews.
[254] Industry interviews.
[255] Industry interviews.
[256] Industry interviews.
[257] Industry interviews.
[258] Investigative Consultants, "Florencia 13 Gang Member Arrested in Piracy Case," *IP Crimes*, Oct. 2010, 8.
[259] Industry interviews.
[260] Investigative Consultants, "Florencia 13 Gang Member Arrested in Piracy Case," 8.
[261] Investigative Consultants, "Florencia 13 and White Fence Gang Members Arrested," 8.
[262] See, e.g., Deputy Secretary of Defense William J. Lynn III, "Defending a new domain: The Pentagon's cyber strategy," *United States Cyber Command: Cyber Security*, Sept./Oct. 2010, http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx (accessed 29 Apr. 2011).
[263] DOJ, "Owner and Employee of Florida-based Company Indicted in Connection with Sales of Counterfeit High Tech Devices Destined to the U.S. Military and Other Industries," *Press Release*, 2, http://www.justice.gov/criminal/cybercrime/wrenIndict.pdf (accessed 29 Apr. 2011).
[264] See FBI, "Pirated Software," 4; see also Deputy Secretary of Defense William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy."
[265] BSA, "Software Piracy on the Internet,"; Krebs and Nakashima, "File Sharing Leaks Sensitive Federal Data,"; FBI, "Pirated Software," 4.

[266] FBI, "Pirated Software," 8.
[267] Robert McMillan, "Hackers break into water system network," *Computerworld*, 31 Oct. 2006, http://www.computerworld.com/s/article/9004659/Hackers_break_into_water_system_network
[268] Grow, "Dangerous Fakes."
[269] FBI, "Pirated Software," 9.
[270] FBI, "Pirated Software," 9.
[271] Industry interviews.
[272] DOJ, "Operation Buccaneer: Illegal 'warez' organizations and Internet piracy," http://www.cybercrime.gov/ob/OBorg&pr.htm (accessed 13 May 2011).
[273] Industry interviews.
[274] FBI, "Movie Piracy Tools and Techniques," 7.
[275] See, e.g., DOJ, "Former Intel Employee Indicted for Stealing more than $1 Billion of Trade Secrets," *Press Release*, 5 Nov. 2008, http://www.justice.gov/crimina/cybercrime/paniIndict.pdf (accessed 14 Feb. 2011).
[276] United States Attorney Southern District of New York, "Former employees of fashion industry company charged with computer hacking and trade secret theft charges," *Press Release*, 27 Oct. 2008, http://www.justice.gov/usao/nys/pressreleases/October08/whiteandganttarrest.pr.pdf (accessed 13 Feb. 2011).
[277] United States Trade Representative (USTR), "2011 Special 301 Report," Apr. 2011, 19-41 (2011 Special 301 Report).
[278] USTR, "2011 Special 301 Report," 19.
[279] Central Intelligence Agency (CIA), "China," *The World Factbook*, www.cia.gov/library/publications/the-world-factbook/geos/ch.html (accessed 8 May 2011).
[280] Government interview; U.S. Census Bureau, 2010 Census Data, http://2010.census.gov/2010census/data/ (accessed 8 May 2011).
[281] UNODC, "Globalization of Crime," 10.
[282] CIA, "China," *The World Factbook.*
[283] U.S. Census Bureau, "Top trading partners – Total Trade, Exports, Imports," http://www.census.gov/foreign-trade/statistics/highlights/top/top1012yr.html (accessed 12 May 2011).
[284] Speaker, United States Patent and Trademark Office (USPTO), Global Intellectual Property Academy (GIPA), Seminar on Intellectual Property Issues in China for Government Officials, 28-29 July 2010.
[285] U.S.-China Economic and Security Review Commission (China Commission), "2005 Report to Congress," Nov. 2005, 86, 88, http://www.uscc.gov/annual_report/2005/annual_report_full_05.pdf (accessed 5 May 2011).
[286] China Commission, "2005 Report to Congress," 86.
[287] China Commission, "2010 Report to Congress," Nov. 2010, 13-14, http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf (accessed 5 May 2011); China Commission, "2005 Report to Congress," 85.
[288] Richard Freemen, National Bureau of Economic Research, "Does Globalization of the Scientific/Engineering Workforce Threaten U.S. Economic Leadership?," *Working Paper 11457*, June 2005, 9.
[289] United States International Trade Commission (ITC), "China: Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy," Nov. 2010, 5-1, http://www.usitc.gov/publications/332/pub4199.pdf (accessed 4 May 2011).
[290] China Commission, "2010 Report to Congress," 48 (citing U.S. Chamber of Commerce James McGregor, "China's Drive for 'Indigenous Innovation': a Web of Industrial Policies (Washington, D.C.: U.S. Chamber of Commerce, 28 July 2010), 4).
[291] ITC, "China: Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy," 5-2.
[292] USTR, "2010 Special 301 Report," 30 Apr. 2010, 9, http://www.ustr.gov/webfm_send/1906 (accessed 4 May 2011).
[293] Government interview; Industry interview.
[294] Industry interviews.
[295] Industry interview; Government interview.
[296] Report of China TDY Team.
[297] Government interview.
[298] Industry interview.
[299] Industry interview.
[300] IACC, "Negative Consequences," 19.

[301] Doug Palmer and Melanie Lee, "Special Report: Faked in China: Inside the Pirates' Web," *Reuters*, 26 Oct. 2010, www.moneycontrol.com/news/features/fakedchina-insidepiratesweb_494163.htmal (Faked in China).
[302] Industry interview.
[303] China Commission, "2005 Report to Congress," 87.
[304] Robert Slate, "Competing With Intelligence: New Directions in China's Quest For Intangible Property and Implications For Homeland Security," *Homeland Security Affairs*, Vol. V, No.1, January 2009.
[305] Intelligence Science Board, "The Intelligence Community and Science and Technology: The Challenge of the New S&T Landscape," *Task Force Report*, (Washington, DC: DNI, Nov. 2006) 27-28 (ISB Report) (citing Richard Silberglitt, et. al., *The Global Technology Revolution 2020, In-Depth Analyses* (Santa Monica, Calif.: The RAND Corporation, 2006)), http://www.fas.org/irp/dni/isb/landscape.pdf (accessed 19 Apr. 2011).
[306] China Commission, "2005 Report to Congress," 93.
[307] China Commission, "2005 Report to Congress," 93 (citing Damian McElroy, "China Aims Spy Network at Trade Secrets in Europe," *The Telegraph*, 3 July 2005).
[308] China Commission, "2005 Report to Congress," 93.
[309] ISB Report, 9-10 (citing Counterintelligence in the Time of Rapid Change: The Impact of Technology and Globalization, 26 June 2006).
[310] FBI, "Theft of Trade Secrets 2009: Potential Targeting by Chinese Actors," 8 Mar. 2010, 7.
[311] Erin Swike, Sean Thompson, and Christine Vasquez, "Piracy in China," *Business Horizons*, 2008, 51.6, 493-500 (Piracy in China).
[312] China Commission, "2009 Report to Congress," Nov. 2009, 167, (citing Demetri Sevastopulo, "Chinese hacked into Pentagon," *Financial Times*, 3 Sept. 2007) http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf (accessed 5 May 2011).
[313] China Commission, "2009 Report to Congress," 167 (citing Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, 21 Apr. 2009).
[314] China Commission, "2010 Report to Congress," 237-38.
[315] China Commission, "2010 Report to Congress," 15.
[316] David Drummond, Google, "A new approach to China: an update," *The Official Google Blog*, 22 Mar. 2010, http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html (accessed 29 Apr. 2011).
[317] China Commission, "2010 Report to Congress," 237-38.
[318] See, e.g., DOJ, "New Indictment Expands Charges Against Former Lucent Scientists Accused of Passing Trade Secrets to Chinese Company," *Press Release*, 11 Apr. 2002, www.justice.gov/criminal/cybercrime/lucentSupIndict.htm; DOJ, "Citizen of the People's Republic of China Indicted in Scheme to Steal Trade Secrets," *Press Release*, 24 Sept. 2009, www.justice.gov/usao/nj/Press/files/pdffiles/2009/zhu0924%20rel.pdf (accessed 13 May 2011).
[319] See, e.g., DOJ, "Two Engineers Found Guilty of Stealing Goodyear Trade Secrets,"
[320] See, e.g., DOJ, "Former Boeing Engineer Sentenced to Nearly 16 Years in Prison For Stealing Aerospace Secrets For China," *Press Release*, 8 Feb. 2010, www.justice.gov/criminal/cybercrime/chungsent.pdf (accessed 13 May 2011); DOJ, "Chinese Chemist Convicted in Theft of Trade Secrets," *Press Release*, 16 May 2008, www.justice.gov/criminal/cybercrime/zengConvict.pdf (accessed 13 May 2011).
[321] See, e.g., DOJ, "Chinese National Sentenced Today For Stealing Ford Trade Secrets," *Press Release*, 12 Apr. 2011, www.justice.gov/criminal/cybercrime/yusent2.pdf (accessed 13 May 2011).
[322] See, e.g., DOJ, "Former Dow Research Scientist Convicted of Stealing Trade Secrets and Perjury," *Press Release*, 7 Feb. 2011, www.justice.gov/opa/pr/2011/February/11-crm-156.html (accessed 13 May 2011).
[323] Symantec Corp., "More Than Half of Ex-Employees Admit to Stealing Company Data;" FBI, "Theft of Trade Secrets 2009," 9.
[324] See, e.g., DOJ, "Chinese Chemist Convicted in Theft of Trade Secrets," *Press Release*, 16 May 2008, http://www.justice.gov/criminal/cybercrime/zengConvict.pdf
[325] See, e.g., Tian v. Holder, No. 08-3391, (8th Cir. 19 Aug. 2009), http://caselaw.findlaw.com/us-8th-circuit/1037071.html (accessed 13 May 2011).
[326] Industry interview.
[327] Government interview.
[328] Industry interviews; Government interviews.
[329] Palmer and Lee, "Faked in China."
[330] USTR, "2010 Special 301 Report," 10.
[331] Palmer and Lee, "Faked in China."

[332] OECD, "2008 Report," 66.
[333] UNODC, "Globalization of Crime," 10.
[334] USTR, "2010 Special 301 Report," 19.
[335] Industry interview.
[336] Industry interview.
[337] Industry interview.
[338] Industry interview.
[339] Industry interview.
[340] Palmer and Lee, "Faked in China."
[341] CBP and ICE, "Intellectual Property Rights Fiscal Year 2010 Seizure Statistics – Final Report," 10.
[342] CBP and ICE, "Intellectual Property Rights Fiscal Year 2010 Seizure Statistics – Final Report," 16.
[343] CBP and ICE, "Intellectual Property Rights Fiscal Year 2009 Seizure Statistics – Final Report," 9.
[344] Industry interview.
[345] Government interviews.
[346] Swike, et al., "Piracy in China," (citing D. Chow, "Intellectual Property protection as economic policy: Will China ever enforce its IP laws?" 16 May 2005).
[347] USTR, "Out-of-Cycle Review of Notorious Markets," 28 Feb. 2011, 5, http://www.ustr.gov/webfm_send/2595 (accessed 12 May 2011).
[348] Report of China TDY Team.
[349] Report of China TDY Team.
[350] USTR, "2010 Special 301 Report," 19.
[351] U.S.-China Business Council, "2011 Special 301 Review," submission of the U.S.-China Business Council, 15 Feb. 2011, 2, http://www.uschina.org/public/documents/2011/ustr_special_301_review.pdf (accessed 12 May 2011).
[352] IIPA, "IIPA's 2010 Special 301 Report," Appendix A, 1.
[353] IIPA, "IIPA's 2010 Special 301 Report," Appendix A, 1.
[354] USTR, "2010 Special 301 Report," 19.
[355] Swike, et al., "Piracy in China."
[356] IIPA, "IIPA's 2010 Special 301 Report," Appendix A, 1.
[357] Swike, et al., "Piracy in China."
[358] Swike, et al., "Piracy in China."
[359] Government interview.
[360] Swike, et al., "Piracy in China," (citing BBC News, "China 'fake milk' scandal deepens," 22 Apr. 2004).
[361] Swike, et al., "Piracy in China."
[362] See, e.g., Government interview; Industry interview
[363] USTR, "2010 Special 301 Report," 19.
[364] Government interview.
[365] See, e.g., Swike, et al., "Piracy in China" (China passed two resolutions to protect Olympics symbols); see also Government interview.
[366] USTR, "2010 Special 301 Report," 20.
[367] Swike, et al., "Piracy in China."
[368] Academia interview.
[369] USTR, "2010 Special 301 Report," 22.
[370] USTR, "2010 Special 301 Report," 23.
[371] Swike, et al., "Piracy in China."
[372] Industry interview; Government interview
[373] Industry interviews; Government interviews.
[374] Industry interview.
[375] U.S.-China Business Council, "2011 Special 301 Review," 1.
[376] See, e.g., China Commission, "2009 Report," 34; Speaker, USPTO, GIPA, Seminar on Intellectual Property Issues in China for Government Officials.
[377] China Commission, "2009 Report," 33-34.
[378] China Commission, "2009 Report," 33-34.
[379] Industry interview.
[380] Industry interview; Speaker, USPTO, GIPA, Seminar on Intellectual Property Issues in China for Government Officials.

[381] Government interview.
[382] Government interviews.
[383] Industry interview, Government interviews.
[384] Government interview.
[385] Industry interview.
[386] Government interview.
[387] Transparency International, "Corruption Perceptions Index 2011 Results," China, www.transparency.org/policy_research/surveys_indices/cpi/2010/results (accessed 11 May 2011).
[388] Minxin Pei, "Corruption Threatens China's Future," *Carnegie Endowment for International Peace, Policy Brief No. 55*, Oct. 2007, 1.
[389] Minxin Pei, "Corruption Threatens China's Future," 2.
[390] Minxin Pei, "Corruption Threatens China's Future," 4.
[391] Minxin Pei, "Corruption Threatens China's Future," 6.
[392] Fred Vogelstein, "How Intel Got Inside," *Fortune*, 4 Oct. 2004, http://money.cnn.com/magazines/fortune/fortune_archive/2004/10/04/8186798/index.htm (accessed 5 May 2011).
[393] Industry interview.
[394] Industry interview.
[395] Industry interview.
[396] Doug Palmer and Melanie Lee, "Special Report: Faked in China: Inside the Pirates' Web."
[397] Attendee, Foreign Law Enforcement Community in China meeting, 26 Aug. 2010.
[398] Industry interview.
[399] Industry interview.
[400] U.S.-China Business Council, "2011 Special 301 Review," 1.
[401] U.S.-China Business Council, "2011 Special 301 Review," 1-2.
[402] Government interview; Speaker, USPTO, GIPA, Seminar on Intellectual Property Issues in China for Government Officials.
[403] Industry interview; Speaker, USPTO, GIPA, Seminar on Intellectual Property Issues in China for Government Officials.
[404] Speaker, USPTO, GIPA, Seminar on Intellectual Property Issues in China for Government Officials.
[405] Government interview.
[406] Speaker, USPTO, GIPA, Seminar on Intellectual Property Issues in China for Government Officials.
[407] Academia interview.
[408] "Global 500 2010," *Fortune*, 26 July 2010, http://money.cnn.com/magazines/fortune/global500/2010/countries/China.html (accessed 12 May 2011).
[409] "Huawei, ZTE Was Counterfeit Trademark Huizhou," *China Daily*, 31 Dec. 2010, http://www.china-daily.org/Scientific-News/Huawei-ZTE-was-counterfeit-trademark-Huizhou/ (accessed 13 May 2011); Academia Interview; Robert Slate, "Competing With Intelligence: New Directions in China's Quest For Intangible Property and Implications For Homeland Security;" Industry interview.
[410] Academia interview; Government interview; Speaker, USPTO, GIPA, Seminar on Intellectual Property Issues in China for Government Officials.
[411] Industry interviews.
[412] Swike, et al., "Piracy in China."
[413] ICE, "U.S. and China to Enhance Information Sharing," *Press Release*, 14 Sept. 2010, http://www.ice.gov/news/releases/1009/100914beijing.htm.
[414] United States Department of Commerce, 21st U.S.-China Joint Commission on Commerce And Trade Fact Sheet, http://www.commerce.gov/node/12467 (accessed 12 May 2011).
[415] Industry interviews, Government interviews.
[416] Industry interview.
[417] Government interview.
[418] Government interview; Speaker, USPTO, GIPA, Seminar on Intellectual Property Issues in China for Government Officials.
[419] Industry interview.
[420] Government interview; Speaker, USPTO, GIPA, Seminar on Intellectual Property Issues in China for Government Officials.

[421] Japan External Trade Organization (JETRO), "Spotlight Interview: John Kakinuki on the progress of Japan's intellectual property rights system," Dec. 2005, www.jetro.org/content/324 (accessed 5 May 2011); See also Keisen Associates, "Japanese Intellectual Property Rights (IPR): Where Is It Heading?" 12 May 2009, http://www.keisenassociates.com/05.12.2009(IPSH).htm (accessed 11 May 2011).
(noting creation of Japan's IP Strategy Headquarters in 2003 to help Japan become an "IP-based nation."); Shengliang Deng, Pam Townsend, Maurice Robert, Normand Quesnel, "A Guide to Intellectual Property Rights in Southeast Asia and China," *Business Horizons*, Nov.-Dec. 1996 (Japan previously disregarded IPR legislation until it began to adapt Western technologies that it wanted to protect).
[422] Government interviews; Industry interviews.
[423] USTR, "2011 Special 301 Report," 28.
[424] U.S. Department of State, "Background Notes: Economy," *India*, http://www.state.gov/r/pa/ei/bgn/3454.htm (accessed 13 May 2011).
[425] U.S. Census Bureau, Foreign Trade, "U.S. Imports from India by 5-digit End-Use Code 2002-2010," http://www.census.gov/foreign-trade/statistics/product/enduse/imports/c5330.html (accessed 5 May 2011).
[426] U.S. Census Bureau, Foreign Trade, "U.S. Imports from India by 5-digit End-Use Code 2002-2010."
[427] Government interviews.
[428] Government of India, Ministry of External Affairs, http://www.indianbusiness.nic.in/industry-infrastructure/industrial sectors/drug-pharma.htm (accessed 20 Apr. 2011).
[429] Government interviews; Industry interviews.
[430] U.S. Census Bureau, Foreign Trade, "U.S. Imports from India by 5-digit End-Use Code 2002-2010."
[431] Industry interview.
[432] Government interview.
[433] Calculations using data from CBP and ICE, "Intellectual Property Rights Fiscal Year 2009 Seizure Statistics – Final Report," 8, 13; Calculations using data from CBP and ICE, "Intellectual Property Rights Fiscal Year 2010 Seizure Statistics – Final Report,"13, 16.
[434] CBP and ICE, "Fiscal Year 2010 Seizure Statistics," 16.
[435] KPMG, "Combating Counterfeiting and Grey Market – A Challenge for Indian Corporates," 22 Dec. 2008, 13.
[436] Report from India TDY Team; Government interview.
[437] Government interview.
[438] Roger Bate, "India's Fake Drugs Are a Real Problem," *The Wall Street Journal*, 19 May 2010, http://online.wsj.com/article/SB10001424052748703315404575249901511960396.html (accessed 24 Mar. 2011).
[439] KPMG, "Combating Counterfeiting and Grey Market – A Challenge for Indian Corporates," 6.
[440] IIPA, "2010 Special 301 Report," India, 38.
[441] BSA, "09 Piracy Study," Table 3.
[442] Industry interview.
[443] Government interview.
[444] IIPA, "2010 Special 301 Report," India, 38.
[445] Business of Cinema, "Mumbai Police Seizes Pirated DVDs of Latest Films Worth Rs 85 Lakhs," 3 Dec. 2010, http://businessofcinema.com/news.php?newsid=17396 (accessed 4 May 2011).
[446] Industry interview.
[447] See, e.g. IIPA, "2010 Special 301 Report," 40; Government interview.
[448] FBI, "Intellectual Property Rights: China, India, Russia, and the Tri-Border Area," *Intelligence Study*, 5 Apr. 2011, 15 (IPR: China, India, Russia, and the TBA).
[449] Report from India TDY team.
[450] Industry interview.
[451] Government interview.
[452] KPMG, "Combating Counterfeiting and Grey Market – A Challenge for Indian Corporates," 8.
[453] Government interview.
[454] CBP and ICE, "Fiscal Year 2009 Seizure Statistics," 13; CBP and ICE, "Fiscal Year 2010 Seizure Statistics," 17.
[455] Industry interview.
[456] RAND Corporation, "Film Piracy," 91.
[457] IPR Center, "IP Crime Threats," 8.
[458] Industry interviews; Government interviews.
[459] Transparency International, "Corruption Perceptions Index 2011 Results," India.
[460] Government interview.

[461] Government interview.
[462] OECD, "2008 Report," 370.
[463] Government interview.
[464] Industry interview.
[465] USTR, "2011 Special 301 Report," 28-29.
[466] Government interview.
[467] Government interview.
[468] OECD, "2008 Report," 234.
[469] US DOJ, "Pro-IP Act First Annual Report 2008-2009," 13 Oct. 2009, 18-19, http://www.justice.gov/criminal/cybercrime/proipreport2009.pdf
[470] Government interview.
[471] Rama Lakshmi, "India's market in generic drugs also leads to counterfeiting," *The Washington Post*, 11 Sept. 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/10/AR2010091003435.html (accessed 11 May 2011).
[472] USTR, "2011 Special 301 Report," 25.
[473] U.S. Department of State, "Background Note: Russia," 16 Mar. 2011, http://www.state.gov/r/pa/ei/bgn/3183.htm#econ (accessed 5 May 2011).
[474] U.S. Department of State, "Background Note: Russia."
[475] U.S. Census Bureau, Foreign Trade, "Trade in Goods with Russia: 2010," 2010, http://www.census.gov/foreign-trade/balance/c4621.html#2010 (accessed 5 May 2011);
U.S. Census Bureau, Foreign Trade, "U.S. Imports from Russia by 5-digit End-Use Code 2002-2010," http://www.census.gov/foreign-trade/statistics/product/enduse/imports/c4621.html (accessed 5 May 2011).
[476] U.S. Census Bureau, Foreign Trade, "Trade in Goods with Russia: 2010;" U.S. Census Bureau, Foreign Trade, "U.S. Imports from Russia by 5-digit End-Use Code 2002-2010."
[477] USTR, "2010 Special 301 Report," 23.
[478] MPA and L.E.K., "The Cost of Movie Piracy," 6-7.
[479] IIPA, "2010 Special 301 Report," 122.
[480] IIPA, "2010 Special 301 Report," 128.
[481] IIPA, "2010 Special 301 Report," 96.
[482] IIPA, "2010 Special 301 Report," 16.
[483] IIPA, "2010 Special 301 Report," 96.
[484] IIPA, "2010 Special 301 Report," 129.
[485] IIPA, "2010 Special 301 Report," 95.
[486] IIPA, "2010 Special 301 Report," 23.
[487] IIPA, "2010 Special 301 Report," 93.
[488] IIPA, "2010 Special 301 Report," 92.
[489] USTR, Out-of-Cycle Review of Notorious Markets, 28 Feb. 2011, 3, http://www.ustr.gov/webfm_send/2595 (accessed 13 May 2011).
[490] BSA, "09 Piracy Study," May 2010, Table 3.
[491] IIPA, "2010 Special 301 Report," Appendix A.
[492] IIPA, "2010 Special 301 Report," 128.
[493] FBI, "IPR: China, India, Russia, and the TBA," 21.
[494] IPR Center, "IP Crime Threats," 6-7.
[495] IIPA, "2010 Special 301 Report," 88.
[496] Government interview.
[497] Government interview; USTR, "2010 Special 301 Report," 23.
[498] Transparency International, "Corruption Perceptions Index 2011 Results," Russia, www.transparency.org/policy_research/surveys_indices/cpi/2010/results (accessed 11 May 2011).
[499] IIPA, "2010 Special 301 Report," 95.
[500] Government interview.
[501] IIPA, "2010 Special 301 Report," 124.
[502] Government interview.
[503] IIPA, "2010 Special 301 Report," 123-24.
[504] USTR, "2010 Special 301 Report," 24; IIPA, "2010 Special 301 Report," 129.
[505] OECD, "2008 Report," 247; USTR, "2010 Special 301 Report," 30 Apr. 2010, 24.

[506] OECD, "2008 Report," 248.
[507] OECD, "2008 Report," 248; USTR, "2010 Special 301 Report," 24.
[508] William Smale, "Downturn gives Hollywood bad dreams," *BBC News Business*, 17 Feb. 2011, http://www.bbc.co.uk/news/business-12460222. See also IIPA, "2011 Special 301 Report," 90.
[509] FBI, "IPR: China, India, Russia, and the TBA," 2.
[510] USTR, "2011 Special 301 Report," 27, 32, 43.
[511] Government interviews.
[512] Government interviews.
[513] See World Trade Organization, "Argentina," Trade Profiles, Mar. 2011, http://stat.wto.org/CountryProfile/WSDBCountryPFView.aspx?Language=E&Country=AR (accessed 11 May 2011); World Trade Organization, "Brazil," Trade Profiles, Mar. 2011, http://stat.wto.org/CountryProfile/WSDBCountryPFView.aspx?Language=E&Country=BR (accessed 11 May 2011); World Trade Organization, "Paraguay," Trade Profiles, Mar. 2011, http://stat.wto.org/CountryProfile/WSDBCountryPFView.aspx?Language=E&Country=PY (accessed 11 May 2011).
[514] Data from CBP and ICE seizure records.
[515] U.S. Census Bureau, "U.S. Imports from Brazil by 5-digit End-Use Code 2002-2009," http://www.census.gov/foreign-trade/statistics/product/enduse/imports/c3510.html (accessed 22 Feb. 2011).
[516] IIPA, "IIPA's 2010 Special 301 Report," Appendix A, 1.
[517] IIPA, "International Intellectual Property Alliance 2008 Special 301 Report," 11 Feb. 2008, Appendix A, 2, http://www.iipa.com/pdf/2008SPEC301LOSSLEVEL.pdf (accessed 13 May 2011).
[518] Hudson, "Terrorist and Organized Crime Groups in the TBA," 30.
[519] Hudson, "Terrorist and Organized Crime Groups in the TBA," 30, 74-75.
[520] FBI, "IPR: China, India, Russia, and the TBA," 25.
[521] FBI, "IPR: China, India, Russia, and the TBA," 25.
[522] Government interview.
[523] Government interview.
[524] Government interview.
[525] Government interview.
[526] OECD, "2008 Report," 69.
[527] OECD, "2008 Report," 40, 47, 50; Frontier Economics, "Estimating Global Impact," 17.
[528] Industry interviews.
[529] Analysis by IPR Threat Report Team.
[530] IACC, "Negative Consequences," 25.
[531] ICE, "LA wholesaler sentenced for trafficking designer goods, search of business turned up thousands of counterfeit handbags, shoes, and other apparel," *News Releases*, 22 June 2009, http://www.ice.gov/news/releases/0906/090622losangeles.htm (accessed 2 May 2011).
[532] Industry interviews.
[533] Frontier Economics, "Estimating Global Impact," 13.
[534] FBI, "Theft of Trade Secrets 2009," 5.
[535] Government interview.
[536] Industry interview.
[537] Industry interview; Government interview; Leanne Suter, "Massive Counterfeit Goods Raid at Santee Alley," *ABC Southland News*, 30 Nov. 2007, http://abclocal.go.com/kabc/story?section=news/local&id=5804966 (accessed 2 May 2011).
[538] ICE, "Tampa Super Bowl t-shirt counterfeiter sentenced to 6 months in prison," *News Release*, 5 Mar. 2010, http://www.ice.gov/news/releases/1003/100305tampa.htm (accessed 2 May 2011).
[539] ICC CIB, "The International Anti-Counterfeiting Directory 2009," 25.
[540] Grow, et al., "Dangerous Fakes."
[541] Industry interview; Government interview.
[542] Industry interviews.
[543] European Commission – Taxation and Customs Union, "Report on EU Customs Enforcement of Intellectual Property Rights: Results at the EU Border – 2009," 26.
[544] European Commission – Taxation and Customs Union, "Report on EU Customs Enforcement of Intellectual Property Rights: Results at the EU Border – 2008," Annex 4, 24,

http://ec.europa.eu/taxation_customs/resources/documents/customs/customs_controls/counterfeit_piracy/statistics/2009_statistics_for_2008_full_report_en.pdf (accessed 2 May 2011).
[545] European Commission – Taxation and Customs Union, "Report on EU Customs Enforcement of Intellectual Property Rights: Results at the EU Border – 2007," Annex 4, 20.
[546] Frontier Economics, "Estimating Global Impact," Annex 1.
[547] Recording Industry Association of America, "The Volume of Music Acquired Without Payment," 11.
[548] Siwek, Stephen E. "The True Cost of Sound Recording Piracy to the U.S. Economy," 8.
[549] MPA and L.E.K., "The Cost of Movie Piracy," 5.
[550] Executive Office of the President of the United States, "2010 IPEC Annual Report," 4.
[551] Executive Office of the President of the United States, "2010 IPEC Annual Report," 7.
[552] ICE, "ICE seizes 82 website domains involved in selling counterfeit goods as part of Cyber Monday crackdown," *News Release*, 29 Nov. 2010, http://www.ice.gov/news/releases/1011/101129washington.htm (accessed 29 Apr. 2011); Executive Office of the President of the United States, "2010 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement," 42; DOJ, "Departments of Justice and Homeland Security Announce 30 Convictions, More than $143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware," *Press Release*, 6 May 2010, http://www.justice.gov/criminal/cybercrime/ashoorConvict.pdf (accessed 26 Apr. 2011).
[553] Industry interviews.
[554] Industry interview.
[555] Industry interviews.