THE INFORMATION SOCIETY
2016, VOL. 32, NO. 4, 256–268
http://dx.doi.org/10.1080/01972243.2016.1177762

Routledge
Taylor & Francis Group

# Intellectual property theft and national security: Agendas and assumptions

Debora Halbert

Department of Political Science, University of Hawai'i at Mānoa, Honolulu, Hawai'i, USA

**ABSTRACT**

About a decade ago, intellectual property started getting systematically treated as a national security threat to the United States. The scope of the threat is broadly conceived to include hacking, trade secret theft, file sharing, and even foreign students enrolling in American universities. In each case, the national security of the United States is claimed to be at risk, not just its economic competitiveness. This article traces the U.S. government's efforts to establish and articulate intellectual property theft as a national security issue. It traces the discourse on intellectual property as a security threat and its place within the larger security dialogue of cyberwar and cybersecurity. It argues that the focus on the theft of intellectual property as a security issue helps justify enhanced surveillance and control over the Internet and its future development. Such a framing of intellectual property has consequences for how we understand information exchange on the Internet and for the future of U.S. diplomatic relations around the globe.

**ARTICLE HISTORY**
Received 26 November 2014
Accepted 6 September 2015

**KEYWORDS**
Cybersecurity; intellectual property; national security; piracy; securitization

Articulation of intellectual property (IP) as a threat to U.S. national security (as opposed to economic security) is relatively new and only tangentially discussed in the literature on intellectual property (which is primarily focused on legal analysis) or the literature on cybersecurity (which deals with the concept of IP uncritically). The discourse that advances IP as a national security issue makes two important narrative moves. First, it blurs the lines between domestic economic innovation and the production of classified information. Second, it asserts that other states (with a focus on China) are responsible for the theft of IP, and not just hackers, criminals, and commercial enterprises.

Contrary to the uncritical acceptance that the theft of IP constitutes a national security threat, this article interrogates treatment of IP as a national security issue and thereby a justification for enhancing security in cyberspace. It argues that despite lack of clarity on the part of security analysts and government officials about what IP actually is, the theft of IP is being used to legitimize the presence of U.S. national security interests in the new "operational domain" of cyberspace (Uzal et al. 2014, 407).

In making this argument, this article does not question the threat of cyberattacks (or the threat of attacks) on U.S. computer infrastructure; such attacks are well documented and of concern (Deibert 2013; Deibert and Rohozinski 2010). It instead argues that use of IP to justify enhanced cybersecurity should be examined critically. The politics of creating a new "discourse of danger" (Campbell 1998) will have long-term ramifications for open access to knowledge and alternative models of innovation. The theft of intellectual property framed as a national security issue allows the U.S. government to justify enhanced surveillance and control over the Internet in the name of protecting American information assets, now defined as intellectual property. Such a framing, however, has consequences for future information exchange on the Internet, as well as for the future of U.S. diplomatic relations around the globe.

More broadly, in building up the moral panic around IP theft and using this theft as a justification for enhanced national security measures in cyberspace, the U.S. government endorses a way of thinking about information, development, and nationalism that sees almost all exchange of information as threatening. Manjikian observes that where the utopian, and to some degree the liberal, approach to the Internet sees information sharing as a larger good, the realist sees information sharing as a threat (Manjikian 2010). In making IP a security threat, the realists are establishing the rhetorical stage for the dominance of their interpretation of cyberspace.

This article is structured as follows. The next section traces the articulation of IP as a national security issue by examining the available public documents, including cybersecurity reports issued by the White House, security

**CONTACT** Debora Halbert halbert@hawaii.edu Department of Political Science, University of Hawai'i at Mānoa, 2424 Maile Way, Saunders 640, Honolulu, HI 96822, USA.

agencies, and other players. The subsequent section unpacks the concept of IP and shows why it is problematic to treat it as a national security threat. The final section situates this discourse in the larger debate on U.S. cybersecurity and investigates the implications of treating IP theft as a national security threat.

## The convergence of intellectual property and national security

Ronald Reagan's National Security Decision Directive 145 noted that "Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation" (Reagan 1984). While it does not carry the language of intellectual property that is central to cybersecurity claims today, this early directive advances the convergence of private industry and public national security.

In 2003 the Bush administration issued the first "National Strategy to Secure Cyberspace" report, the document that set the stage for merging issues of cyberspace with those of national security.[1] It focused primarily upon the potential harms caused by insecure networks and security flaws, especially in computerized systems controlling our nation's critical infrastructure (The White House 2003). While intellectual property was mentioned, it was not yet central to the articulation of cybersecurity in a post-9/11 world.

Toward the end of the Bush administration, the Center for Strategic and International Studies (CSIS) issued a "Report to the 44th President of the United States on Cybersecurity." This report raised the crucial cybersecurity issues the next president of the United States would need to address. It noted that as of 2008, despite over a decade of evolution and growth of the Internet, its national security implications had yet to be fully discussed or developed. Specifically, "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2008" (Langevin et al. 2008, 11). Thus, recommendations to the new president set the stage for a more comprehensive approach to national cybersecurity. To emphasize the importance of IP, the authors argued that:

> The immediate risk lies with the economy. Most companies' business plans involve the use of cyberspace to deliver services, manage supply chains, or interact with customers. Equally important, intellectual property is now stored in digital form, easily accessible to rivals. Weak cybersecurity dilutes our investment in innovation while subsidizing the research and development efforts of foreign competitors. In the new global competition, where economic strength and technological leadership are as important to national power as military force, failing to secure cyberspace puts us at a disadvantage. (Langevin et al. 2008, 11)

The report never provides a definition of intellectual property in use except to say this "property" is stored on computers and thus more vulnerable than before.[2]

What is significant is that intellectual property generally described, which is vital to our economic strength, is deemed as important as military force.[3] The report goes even further, saying this is "a strategic issue on par with weapons of mass destruction and global jihad" (Langevin et al. 2008, 15). Here we see just how far the policy discourse on IP moved from early economic concerns to those of national security. The CSIS report, including language on the importance of intellectual property, was cited in one of President Obama's first forays into cyberspace policy—his 2009 "Cyberspace Policy Review" (The White House 2009).

President Obama took up the call of cybersecurity and has made addressing the theft of intellectual property a top priority. In the May 2011 report "International Strategy for Cyberspace," the follow-up to the 2003 Bush administration report, Obama details the threat facing the United States in this integrated and networked world.[4] The report lists several principal cyber threats to national security—cyberattacks that disrupt service; criminal behaviors such as fraud, identity theft, and child exploitation that undermine trust in the digital world; and theft of intellectual property that "threatens national competitiveness and the innovation that drives it" (Obama 2011, 4). According to the report, these challenges emerge because the anonymity of the Internet creates "safe havens" for criminals who pose cybersecurity threats that can even "endanger international peace and security" (Obama 2011, 4). In other words, the anonymity of the Internet, which is celebrated in many quarters, is now also a threat to the U.S. government.

In contrast to those calling for collective determination of cyber norms premised upon prevailing social norms (Mueller, Mathiason, and Klein 2007; Hurwitz 2015; Svensson and Larsson 2012; Larsson 2013), this report establishes government mandated international norms that respect intellectual property. Furthermore, the report goes on to outline the U.S. response should the norms now articulated be violated. Specifically, the United States will first continue to pursue diplomacy, it will also work to dissuade potential actors from engaging in norm violating behavior, and, finally, the United States will seek to deter any possible threat to its national and economic security (Obama 2011). The report is clear that violence is an acceptable response to threats to U.S. cybersecurity. It notes that:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. (Obama 2011, 12)

Also in 2011, the Office of the National Counterintelligence Executive issued its report to Congress covering acts of economic espionage for the 2009–2011 period (Office of the National Counterintelligence Executive 2011). This report provides specific examples of industrial and economic espionage and defines what constitutes the theft of trade secrets. While often overlooked in discussions of intellectual property (that focus primarily on copyrights, patents, and trademarks), trade secrets are a protected form of IP nationally and internationally via the TRIPS (The Agreement on Trade-Related Aspects of Intellectual Property Rights) agreement; Pooley 2013). The 2011 report focuses upon industrial espionage in cyberspace instead of the general cybersecurity threats discussed in other documents and provides additional justification for government intervention to make the Internet a secure place for business and government.

The report noted that it is difficult to assign value to things stolen from industry computers. After all, how much value should be placed on an internal memo listing business talking points (Office of the National Counterintelligence Executive 2011, 3)? That being said, the report offers several insights into how both industry and government entities perceive IP as a national security issue. First, the report recounts that in a 2010 conference hosted by the Office of the National Counterintelligence Executive (ONCE), it emerged that industry actors did not see a significant difference between "cybercrime—for example, identity theft or the misappropriation of intellectual property such as the counterfeiting of commercial video or audio recordings—and the collection of economic or technology information by intelligence services or other foreign entities" (Office of the National Counterintelligence Executive 2011, 1). In effect, industry saw the theft of their intellectual property as the same thing as the theft of state secrets.

Second, the report discusses what the authors consider to be non-cyber methods of generating valuable knowledge through economic espionage, including the use of open source materials—meaning published information in scholarly journals and websites. Given that increasingly these materials are available via online sources, often with some sort of pay-wall, it is not a huge step to see how the U.S. government could reconfigure hacking an academic database, such as JSTOR, into a crime of industrial espionage.[5] More broadly, however, the notion that even acquiring knowledge through open-source materials can be interpreted as a threat to U.S. economic security implies a significantly different approach to scholarly production than what is found in the academy and the growing open access movement.

Finally, to capitalize on the "hactivist" threat posed by Wikileaks, the report argues that future threats may come from activists seeking to make a lifesaving drug available more cheaply or antiwar activists interested in averting the deployment of a new U.S. weapons system. In either scenario, these activists would leak proprietary information to the public and thus undermine U.S. economic and/or national security. In other words, potential security threats are threats coming from intellectual property violations. These activists, along with the emergence of possible regional state actors, are perceived as possible "game changers" in the increasingly complex world of industrial espionage and U.S. national security

The report of the Office of the National Counterintelligence Executive provided the data for the President's February 2013 national strategy to deal with the theft of U.S. trade secrets (and is attached at the end of the President's document). Focused on industrial and economic espionage, the President's February 2013 report tells the public that the full scope of the U.S. administrative infrastructure will be deployed to fight against IP theft. Gone are the days when the FBI had bigger criminal plots to unravel than intellectual property theft—this is now central in the FBI mission.[6] The report's analysis is limited to trade secrets instead of constructing and using a generic concept of "intellectual property" as a foil against which to pitch an argument for increased cybersecurity. That being said, what constitutes a trade secret in the context of this report and of course in the U.S. assessment of damage done to American industry and national security is *everything that might be held on a computer*. Thus, no matter how banal or irrelevant, as long as it is on a computer, it is a trade secret and must be protected against theft.[7]

While Russia is considered a serious offender in terms of industrial espionage, the reports on trade secrets and cybersecurity all point to China as the most aggressive cybersecurity threat. According to Schmidt and Sanger, recent federal indictments of Chinese hackers were directed at positioning U.S. claims about intellectual property theft at the center of United States–China diplomacy (Schmidt and Sanger 2014). In 2011, Bloomberg reported that at least 760 companies had been hacked, primarily by Chinese sources, calling China's efforts an "undeclared cyber war" (Riley and Walcott

2011). While the reporting was short on specifics, Scott Borg, director of the U.S. Cyber Consequences Unit, noted, "We're talking about stealing entire industries." He said, "This may be the biggest transfer of wealth in a short period of time that the world has ever seen" (Riley and Walcott 2011, online para. 16).[8]

The issue of state-based Chinese hacking emerged again in March 2012 when the Department of Defense issued a press release on what it called "the greatest wealth transfer in history." According to this press release, this wealth transfer resulted from the Chinese hacking of critical resources in U.S. industry, universities, and government (Daniel 2012). Here the security firm Mandiant noted that while it may be possible that the Chinese hackers acted without state sponsorship, by far the most likely scenario is that they were deployed by the Chinese state to appropriate U.S. intellectual property (Mandiant Intelligence Center 2013).

The Commission on the Theft of American Intellectual Property recommended that the national security advisor be designated as the "principle policy coordinator for all actions on the protection of American IP" (Blair and Huntsman 2013, 4). While cybersecurity is already within the scope of the National Security Council mandate, such a designation would shift some of the interests in intellectual property protection from its civilian host in the U.S. Intellectual Property Enforcement Coordinator's office, itself only a few years old, to a new position within the National Security Council.

The Department of Homeland Security (DHS) is also in the picture when issues of cybersecurity and intellectual property converge. While the DHS is a vast federal bureaucracy with widespread duties from border control to domestic terrorism, its recent report to Congress did not leave out the threats posed by intellectual property theft. Acting Secretary Rand in his report to the Senate Committee on Homeland Security and Government Affairs on the State of the Homeland told the committee that the cyberworld is fraught with dangers:

> This is critical, time-sensitive work, because we confront a dangerous combination of known and unknown cyber vulnerabilities, and adversaries with strong and rapidly expanding capabilities. Threats range from denial of service attacks, to theft of valuable trade secrets, to intrusions against government networks and systems that control critical infrastructure. These attacks come from every part of the globe, every minute of every day, and are continually increasing in seriousness and sophistication. (Beers 2013, online para. 66)

Other aspects of the threat to the homeland included hackers testing our networks, the sale of counterfeit goods via the Internet, and ongoing attacks on the network from foreign and domestic sources alike (Beers 2013). These dangers were part of the justification used by the Acting Secretary to request additional funding for DHS in the next fiscal year.

Other reports come closer to linking national security and the protection of American lives to IP theft. Attached to the 2013 report by the Obama administration about trade secret theft is yet another report about the importance of protecting U.S. intellectual property. This report for 2012, part of a yearly endeavor by the Defense Security Service, begins by stating that:

> The stakes are high in the battle against foreign collection efforts and espionage that target U.S. technology, intellectual property, trade secrets, and proprietary information. Our national security relies on our collective success at thwarting these persistent attacks. Every time our adversaries gain access to sensitive or classified information and technology, it jeopardizes the lives of our warfighters, since these adversaries can exploit the information and technology to develop more lethal weapons or countermeasures to our systems. Our national security is also at risk in the potential loss of our technological edge, which is closely tied to the economic success of the cleared contractor community and the well-being of our economy. (Defense Security Service 2012, 5)

The language equivocates between stolen national secrets and whatever is meant here by intellectual property, where trade secrets and proprietary information are separate categories. However, with each report linking intellectual property to the national security state, the importance of intellectual property is enhanced, even as what constitutes intellectual property is never clarified.

The Center for a New American Security also issued a 2013 report on cybersecurity that further enforces the growing link between cybersecurity, national security, and intellectual property theft. The new turn, as the report author Irving Lachow notes, is that an active cyberdefense (ACD) is necessary because the threat now comes from state-sponsored spies and sophisticated criminals who create what he calls an advanced persistent threat (APT) (Lachow 2013, 2). These new threats focus on "stealing intellectual property and defrauding individuals and businesses" (Lachow 2013, 2). It is exclusively the threat to intellectual property that Lachow uses to justify his ACD system in the cyber-engagement zone (CEZ), a system where security forces seek to actively intervene in cyberinvasions as they are happening (Lachow 2013).

Space does not allow me to continue to trace the ongoing development of intellectual property as a security concern and its theft as increasingly central to the U.S. security discourses. One last point must be made. In a TED talk via remote computer, Edward Snowden discussed his reasons for disclosing the scope of NSA spying

and his perspectives on U.S. national security. As someone who has advocated for civil liberties and privacy rights for the individual, Snowden argued that protection of intellectual property justified rejecting NSA efforts to install backdoors in Internet systems. When asked whether we became less secure as a result of such backdoors, he said:

> If we hack a Chinese business and steal their secrets, if we hack a government office in Berlin and steal their secrets, that has less value to the American people than making sure that the Chinese can't get access to our secrets. So by reducing the security of our communications, they're not only putting the world at risk, they're putting America at risk in a fundamental way, because intellectual property is the basis, the foundation of our economy, and if we put that at risk through weak security, we're going to be paying for it for years. (Snowden, 2014)

Protection of United States IP has become the rallying cry for a secure network. The world understood through these reports is not an open system where knowledge is shared for the sake of learning, poverty alleviation, or economic development, but instead one where knowledge is owned and controlled by industrial and state actors and its existence as a secret must be preserved and protected at all costs.

In fact, higher education is being reimagined as a national security threat. The National Bureau of Asian Research's Report on the Commission on the Theft of American Intellectual Property argued that immigrants coming to study in the United States return home to use their "IP knowledge" to compete against the United States (Blair and Huntsman 2013). These students turn into "walking IP" and "take trade secrets with them when they leave" (Blair and Huntsman 2013, 13). More nefarious are foreign students who come to Western higher educational institutions to act as spies for their home countries. The open space of the university may need to be rethought when educating students becomes a threat to national security. However, before we collectively agree that the theft of IP by foreign states is a significant national security threat of the information age, as the reports in this section have claimed, it might be worthwhile to know exactly what is meant by IP and how it has been stolen.

## The new face of IP and national security

The previous section sought to demonstrate that the concept of intellectual property has now been built into the national security discourse justifying a U.S. security role in cyberspace. This section interrogates the inclusion of IP in these reports. To remake IP theft into a security issue, the report authors do not delve into the technical differences between intellectual property regimes such as copyright, patent, trademark, and trade secrets, they do not discuss that this is primarily an economic doctrine designed to facilitate the exchange of ideas, and they do not discuss that copyright and patent law deals with infringement in the context of unauthorized copies or use of an idea, not theft. Instead, these documents reference an abstract notion of "intellectual property" located within the national sphere of the U.S. state. There is little clear thinking or analysis presented that distinguishes between economic threats to private industry and hackers stealing government secrets. Intellectual property itself is never defined in any meaningful detail. The specifics of the actual damage done (given that what is taken is a copy) and how it has impacted innovation or progress are not articulated. Rather, there is an assertion that what has happened constitutes a significant threat to American national security. That threat blurs the distinction between protection of private economic interests and that of the nation-state.

First, the concept of intellectual property is a misnomer that implies something has been stolen when it has not. The scholarship critical of expansion and restrictive control of intellectual property has been well established and the concept itself is contested, including the language of theft associated with it (Lessig 2005; Lessig 2006; Lessig 2002; Doctorow 2008; Stallman, Lessig, and Gay 2002; Halbert 2005; May 2000; Boyle 2003; McLeod 2007; Peñalver and Katyal 2010; Boyle 1996; Bollier 2002; Hemmungs Wirtén 2004; May and Sell 2006; Drahos 2003; Correa 2000; Boldrin and Levine 2008; Stallman 2006; Bettig 1996; Vaidhyanathan 2001). It is difficult to know why the report authors remain ignorant or nonresponsive to the IP policy field they have appropriated, given that the relevant literature has existed for decades. One explanation is that they intentionally equivocate about the different types of IP to enhance the perception of the threat.

Looking more critically at the theft of IP claim, if intellectual property can be stolen, then its theft means some sort of loss has occurred for its owners. However, IP laws protect nonrivalrous goods. Unlike tangible property, multiple people can use IP simultaneously. At its worst, the IP discussed in these reports are copies of work produced by others, but the victims of theft have not been deprived of their original works, unless there is malicious erasing. IP exists to create scarcity in information by imposing limited monopolies on otherwise intangible and easy-to-share expressions and ideas. Thus, the larger question remains, what has been stolen when a "theft" of IP has taken place? Basically, it is the theft of a temporary monopoly over how ideas are shared or, in

some cases here, classified works. Such a vague construction of intellectual property must be challenged. IP theft is substantively different from other forms of theft and the use of the word property to describe these actions conceals as much as it reveals.

If the specific legal codes that fall under the general umbrella term intellectual property were used instead, then it would be possible to determine more clearly what was "stolen." IP is simply a quick way of referring to the multiple legal codes that protect the distinct legal regimes of copyrights, patents, trademarks, and trade secrets. The notion that one could aggregate these disparate rights into a single concept and claim it to be of such significance that our national security depends upon its protection is deeply problematic. By contrast, if what is stolen is trade secrets we might have a better idea of the problem. If, on the other hand, the appropriation is of a trademark and related works, then the national security implications seem unclear. Disaggregation of the "theft of IP" into what type of IP has been threatened can help us better understand what in fact was copied.

Second, as a body of law, IP is primarily economic and public in nature and thus should not be conflated with government secrets or other forms of classified information. In other words, it cannot be divorced from a public process, as the FBI agent who deposited a copy of a secret interrogation manual after registering it with the copyright office found out (Baumann 2013). With the exception of trade secrets and the extension of copyright to unpublished works, IP law grants a limited monopoly to the author or inventor of a work in exchange for public disclosure of the creative work. Secret military documents are valuable to national security, but to call them IP in the conventional sense of this word is inaccurate. In fact, to register a copyright, a copy of the document must be filed with the U.S. copyright office (though copyright is automatically attached upon the fixation of something in a tangible form and without registration, so technically one could call all written work copyrighted). Patents and trademarks go through similar public processes. While inventions can be classified as secret if they are deemed to risk national security, classifying them in such a manner means that the patent is not awarded. Here, while the technology is kept secret, economic potential may be lost. Ironically, if policymakers link economic security to national security, the resulting rendering of some inventions secret could have a significant negative economic impact in the United States (Schulz 2013).

Trade secret laws exist to provide companies with a way of protecting their private knowledge from theft. However, industrial espionage predates the security concern over hackers using computers to steal IP. In the reports analyzed, the examples of industrial spying did not involve hackers but rather the theft of materials by employees—the conventional method of industrial spying.

Third, given the critique of theft in the preceding section, it is unclear how one assesses the economic damage when what is "taken" is intangible and technically not lost. These reports claim that billions of dollars have been stolen as a result of intellectual property theft. For example, in the recent *New York Times* coverage of the Chinese indictment, the Attorney General claimed that the hackers stole 700,000 pages of e-mails from one company, which sounds significant (Schmidt and Sanger 2014). However, how many of these e-mails were of any "value"? How do you assign value to e-mails? Would only the e-mails including technical details count as valuable? It may be that after sifting through 700,000 e-mails, a Chinese innovator will be able to use whatever technical processes have been distilled to create a competitive advantage. The same could be said of the thousands of old scientific articles "stolen" from public libraries in the United States. However, as Thomas Rid argues, "Tacit knowledge is a major challenge for espionage, especially industrial espionage" (Rid 2013, 84). Since taking knowledge is much easier than putting it to use, theft of trade secrets has had a relatively limited impact on competitive economic development (Rid 2013). However, though illegal, theft of trade secrets does not limit the company from which the information was stolen from pursuing its own innovative path.

The underlying assumption in these reports is that foreign governments steal our ideas but then take these ideas and make superior products before we can. Perhaps instead of feeling threatened, it might be worthwhile to ask why American businesses are not bringing their innovations to market more quickly—this is, after all, the entire point of a free-market competitive system. Finally, while this type of "theft" may be of economic concern, blurring it into a national security threat is problematic. These types of distinctions are absent from the policy analysis presented in the statements made about how much the theft of IP costs the United States.

What becomes clear when looking at the confluence of reports and statements from public figures and the relevant think tanks is that without any critical nuance, intellectual property theft has achieved a level of political valence akin to the elusive threat posed by the war on terror. It is likely we can never know what has been "stolen" when the government claims China is stealing our intellectual property, in part because it may be classified information and in part because the vagueness of the claim allows any number of otherwise innocuous items to be counted as stolen. However, there are reasons we

should be concerned about such claims and challenge the wholesale use of the concept of IP to justify national security efforts in cyberspace.

## Why we should care about the securitization of intellectual property theft

Intellectual property has grown in importance since the mid-1990s when it became clear that the networking possibilities of the information age were changing the way people communicated, did business, shared information and much more. As discussed earlier, commercial interests, especially entertainment companies, were among the first to recognize the threat to their business models posed by the Internet. They embarked upon a now decades-long effort to preserve their way of doing business using all possible strategies, from changing the law to educational campaigns advancing a framework of cybernorms that suited their commercial interests.

While it is arguable that the industry has lost anywhere near the amounts of money it claims, what has been successfully accomplished is the uncritical acceptance of the IP theft narrative at all levels of American government as a truth.

The Copenhagen School initially developed securitization theory in the 1990s as a form of critical security studies. A security threat, according to the Copenhagen School, does not exist "naturally" but is instead narrated into being (van Munster 2005, 2). Such an understanding of securitization "follows the recognition that security is socially constructed and politically powerful" (Browning and McDonald 2011, 236). To qualify as a securitizing act, according to the Copenhagen School, three criteria must be met:

> (a) existential threats to the survival of some kind of referent object that (b) require exceptional measures to protect the threatened referent object, which (c) justify and legitimise the breaking free of normal democratic procedures. (van Munster 2005, 3)

Furthermore, to become securitized, an actor must make a securitizing move that is accepted by a target audience and justifies actions that "break the normal political rules of the game" (Buzan et al. 1997, 24).

Over the last two decades, several critiques to the original Copenhagen School paradigm have emerged. Specifically, some argue that a focus on existential threats is too limiting. For an issue to meet the mandates set by securitization theory, an "existential threat" through which new and extraordinary measures must be taken outside conventional politics must exist (Williams 2003). As van Munster points out, while the original articulation of securitization focused upon existential threats, the ongoing war on terror helps us to understand securitizing moves as also articulating the risk of potential threats (van Munster 2005). Cybersecurity is another such threat.

According to Hansen and Nissenbaum, the Copenhagen School rejected the need to theorize cybersecurity as an autonomous security issue in the 1990s (Hansen and Nissenbaum 2009, 1156). Yet the potential risk posed by cyberwar and the underlying and associated risks posed by IP theft are now playing a central role in how the United States articulates its security policy. How the state, accompanied by private security-based actors, constructs a discourse of security surrounding the protection of IP and shifts the security agenda to reflect the new socially constructed threat is important to analyze. Thus, the securitization of IP as traced in the reports discussed here takes an unconventional security threat and translates it into a threat that can be understood using very conventional security language. Cavelty says of cybersecurity that while it may not have been successful as a securitizing move, "what has evolved, however, is a new logic of security (Cavelty 2007, 137). This new logic of security, where cyberspace generally is seen as a national security threat and the theft of intellectual property is understood to be a significant justification for further defending cyberspace, is why we should take the claims made in these reports seriously.

Cavelty is interested not in the securitization move itself, but in the nature of the measures drafted as a result—how a securitizing move leads to policy decisions and countermeasures. This is the focus of "threat politics," which pushes security studies to the next stage (Cavelty 2007, 26). In the case of cyberspace and IP theft, it is worth remarking that state actors have assimilated IP into their justification for defending U.S. territory, this time in cyberspace. This section uncovers why the articulation of IP as a security threat matters in the context of threat politics. Ultimately, by shifting IP into a national security frame, the lines between theft and information sharing are increasingly blurred and the U.S. government positions itself even closer to using cyberspace as a justification for war (virtual or conventional).

One possible justification for the securitization of IP is that it can help mobilize U.S. efforts to enhance military budgets. For example, the Department of Defense now has a "cyber strategy" requiring a buildup of cyber resources and personnel to address the growing threat posed by the cyber domain, including the theft of intellectual property from state and nonstate actors (Carter 2015). In a March 2012 press release, the Department of Defense (DOD) called for increased funding (to $3.4 billion for FY 2013) for a coordinated approach to cybersecurity that involves the DOD, the Department of

Homeland Security, the FBI, and private industry (Daniel 2012). According to General Keith B. Alexander, "Cyber is a team sport, it is increasingly critical to our national and economic security. … The theft of intellectual property is astounding" (Daniel 2012, online para. 8). Thus, IP theft within the new cyberdomain can help justify ongoing defense budgetary allocations.

Despite these efforts to shore up military budgets, cybersecurity is an uneasy fit with the conventional understanding of national security threats. While the reports just described assert unequivocally that the theft of IP is a national security threat, to position IP theft as a national security threat is questionable. For example, the Chinese hacking incident(s) has been instrumental in helping justify increased cybersecurity to protect intellectual property. As Clarke and Knake argue, "Even if a major cyberwar involving the U.S. never happens, Chinese cyber espionage and intellectual property war may swing the balance of power in the world away from America. We need to make protecting this information a much higher priority, and we need to confront China about its activities" (Clarke and Knake 2010, 237). What "intellectual property war" might be in this context is a matter of speculation. What information needs protecting is also unclear, but the concept is broad enough to establish any Chinese knowledge acquisition as a threat. It is argued that the data theft undertaken by the Chinese is specifically designed to improve their military and technological capacities to better compete with the United States (Eun and Abmann 2014). This particular threat is not based upon superior weaponry, but upon superior use of information. In other words, the fear is that China may be smarter than the United States and that the vast downloading of information from U.S. computers will help them achieve international dominance.

More significantly, and what makes the securitization of IP a new rhetorical move worth remarking upon and raising concern about, the Chinese state is now the culprit in this new narrative of IP war. The United States has pointed to China's intellectual property pirates for decades (Halbert 1997; Neigel 2000; Yu 2006; Yu 2005; Mertha 2005). However, the focus has been on the lax enforcement of intellectual property rights that allowed Chinese pirates to make illegal copies of U.S. movies, music, software, and designs. The shift from a failure of the Chinese state to protect U.S. intellectual property (movies, software, music, etc.) to the public accusation by American officials that the Chinese government itself is responsible for intellectual property theft is an important new dimension in the evolution of international intellectual property conflicts.

The state as IP pirate makes for a different set of possible responses in the context of a threat politics—diplomatic and military—and requires a far more vigilant system of surveillance on the part of the United States. If the rhetorical effort to establish IP theft as a concern for American national security is to be taken seriously, where does this logic lead us in terms of future international relations? If virtually all policy treatments of cybersecurity point to the theft of IP as a significant justification for more security, less sharing, and more national vigilance in protecting "our IP," then what kind of future battles does such logic set up?

Among the first to call theft of information a type of warfare was computer scientist Dorothy E. Denning, who included IP theft in her hierarchies of offensive operations that could be conducted in cyberspace (Denning 1998). However, there remain serious questions about whether "cyber" fits the concept of war at all. There is an ongoing debate in security circles on the potential of cyberwar and what it really means (Gartzke 2013; Gjelten 2013; Ophardt 2010; Rid 2012; Farwell and Rohozinski 2012; Sharma 2010; Stevens 2012; Stone 2013; McGraw 2013; Ventre 2011; Singer and Friedman 2014). Jerry Brito and Tate Watkins argue that cyberwar is primarily hype produced by the growing cybersecurity industrial complex, and they suggest that more clear definitions of the threat and more realistic assessments need to be made (Brito and Watkins 2011). Rand senior policy analyst Martin C. Libicki also downplays the significance of what remains primarily a theoretical threat (Libicki 2007). Rid argues that the concept of cyberwar is highly problematic and that, in fact, cyberattacks actually significantly diminish violence instead of enhancing it (Rid 2013).

International law requires a state-actor as the instigator of an act of war, which may not be discernable in a potential cyberwar (Ophardt 2010). The territory under attack, as well as the territory from where the attack originates, may also be unclear, a divide that distinguishes cybercrime from cyberwar in contexts where the two are not deliberately blurred (Hollis 2011). According to Ophardt, we are already seeing glimpses of tomorrow's cyberwars in the dynamic between industry-hired mercenaries and file sharers. The fact that file sharing is being used as an example of the wars of the future does not bode well for demarcation of IP in future conflicts.

We have not yet gone so far as to claim IP theft as an act of war. In the aftermath of the Chinese hacker scandal, the Pentagon issued a report on cybersecurity in which it recommended that some cyberattacks could be considered acts of war, but noted that "routine theft of intellectual property" was "generally" not considered to be in that category (Michaels 2013). The widely discussed *Tallinn Manual on the International Law Applicable to Cyber Warfare* also explicitly excludes protection of private intellectual property from consideration as an

activity governed by the law of armed conflict (Schmitt 2013). It sees the law of armed conflict applicable only when state–state actions are involved. Despite the implications intellectual property theft has for national security, Schmitt does not think it belongs in this domain (Schmitt 2013). However, given that the shift in discourses over the threat to the national security of American IP comes from other states, the lines between protection of commercial and government IP assets are getting ever more blurry. Given the incessant ramping up of the threat posed by IP theft, it is likely that claims regarding IP theft as an act of war are not too far in the future.

Of additional concern is the fact that by making IP theft a national security threat without being clear about what actually constitutes intellectual property, not only does the U.S. government create a new reason for a militarized Internet, but it also sets the stage for companies to assert that a range of other activities from file sharing to producing counterfeit DVDs threaten national security and require further state intervention. Already, private industry has sought to link IP theft to terrorism in an effort to deploy the U.S. security state to defend its business practices (Treverton et al. 2009; Donahue and Hirschmann 2008). Whatever form IP theft might take in the national security configuration, from the unauthorized download of an internal departmental memorandum to counterfeit food production to illegal song downloads, the framing of the policy documents discussed here provides justification for further restriction of the openness of the Internet.

## Conclusion

This article sought to raise concerns about appropriating the concept of IP as a national security issue and using it to justify the protection of cyberspace. The question remains open, however, as to what the U.S. response should be, not only to possible cybercrime but also to cybersecurity more generally. As Clarke and Knake warn, "Countries need to recognize that cyber espionage can easily be mistaken for preparation of the battlefield and that such actions may be seen to be provocative" (Clarke and Knake 2010, 236). Given the fact that the Obama administration reserves the right to respond with force to any credible threat to its security, even in cyberspace, the possibility of military escalation is there.

Despite the current popularity of using the language of IP theft to justify enhanced national security in cyberspace and to expand U.S. military oversight of cyberspace, other justifications for such actions should be sought and IP should remain in the civilian and economic realms. Ultimately, the implications of securitizing IP are significant. As a result of the threat to American national security created by this framing of the theft of IP, more sophisticated cyberdefenses, public/private information sharing, and Internet surveillance are justified. The lines being blurred to promote IP theft as a threat could undermine the basic connective capacity of the Internet itself. Utilizing the Internet to fight an offensive information war will encourage the already existing trend of Internet Balkanization that has been in part motivated by American online spying, as other countries seek to protect themselves from potential cyber threats.

Instead of heightening tension between states over information sharing and setting the stage for future cyberwars over the theft of IP, there could be other possible ways to work through issues of information exchange and possible theft outside the national security/military paradigm. Hollis, for example, suggests that because it is so difficult to identify the origin of a cyberattack, the focus should instead be on constructing a duty to assist in the event of such an attack (Hollis 2011, 209), rather than focusing on the origin of the attack. Such a perspective sees the Internet as a common "international" space, rather than the sovereign domain of nation-states. While the debate over what possible international cybernorms might govern cyberspace is ongoing and few issues have been resolved (Hurwitz 2015), considering an approach where at least minimum international standards not dictated only by U.S. security interests prevail is another possible avenue to diffuse the securitization of IP currently underway. In other words, possibilities other than understanding IP theft as a threat to U.S. national security exist, possibilities where the exchange of information and the benefits of an open Internet still prevail, even when discussing the potential threat China plays (Lindsay 2015).

I have sought to argue that the securitization of IP should be of significant concern, and yet the academic literature on securitization studies may not acknowledge its importance because of the limited way in which that literature defines securitization. One path forward is to engage more critically with the academic literature on securitization studies. While Cavelty's work on threat politics helps provide new avenues for articulating new threats, more can be done in this area. Securitization studies were intended to be critical of mainstream international relations; however, their commitment to theorizing within the constraints of their definitional model limits the application. Thus, one way forward includes a more robust theory of securitization that allows for the discussion of new types of threats in cyberspace.

An additional path forward is to use the analysis of securitizing IP developed here to delve more deeply into the specific cybersecurity examples used by advocates of the securitizing IP school of thought and determine much more clearly what the implications of massive copying of intellectual property are. This article is intended to raise awareness of how the "theft of IP" language is being appropriated to justify enhanced cybersecurity, but space limitations preclude more detailed analysis. Such analysis would build upon the documentation provided here regarding the evolution of a securitizing discourse surrounding the theft of IP.

Finally, understanding the implications of this rhetorical move has very real world applications. These securitizing moves are not academic, but will have real consequences for how the national security state moves forward in cyberspace, how surveillance is justified, how military budgets are constructed, and much more. To that end, the type of information society we wish to inhabit in the future is implicated in the struggles this article has attempted to make visible, and more can be done to articulate the vision of a more positive future regarding how information is shared across national boundaries.

The struggle between open access and proprietary knowledge has been raging for as long as intellectual property laws have existed. The securitization of intellectual property takes the debate to the next level. As the language of national security colonizes the debate about intellectual property, those who would advocate for open access, free sharing of information, and even technology transfers will find themselves with even more limited ground upon which to stand if this narrative move is not resisted. The future is not a bright one when anything shared on a computer might now violate the national security of the United States.

## Notes

1. Hansen and Nissenbaum take cybersecurity through the 2003 National Strategy statement and focus on the computer aspects of cybersecurity (Hansen and Nissenbaum 2009). My work brings the cybersecurity analysis to the present with a focus on the growing importance of intellectual property in generating a securitizing debate over the future of American national security.
2. It reported that the "intellectual property" stolen by foreign sources included designs, blueprints, and business processes that "cost billions of dollars to create"(Langevin et al. 2008, 13). The billions of dollars assessment is not based upon the market value of a product but on how much it costs to create it.
3. The understanding that the private companies are now central to the security of the U.S. infrastructure was further articulated in Obama's 2013 executive order on cybersecurity, where he specifically outlined the need for information sharing between public and private actors. The details regarding how to develop such information sharing are to be worked out (Obama 2013).
4. The recently concluded President's Review Group on Intelligence and Communications Technologies just encouraged President Obama to reaffirm the 2011 report. See Clarke et al. (2013, 22).
5. The United States has already configured the hacking of a database like JSTOR as a threat to domestic security and economic vitality, as its relentless prosecution of Aaron Swartz, leading to his death, shows (Cartalucci 2013; Lessig 2013; Reilly 2013a; Reilly 2013b).
6. The F.B.I. now makes an annual report on its IP-related interventions (Federal Bureau of Investigation 2013).
7. In terms of trade secret theft itself, it is important to note that despite implying that cyber attacks are the greatest threat, every example of trade secret theft produced and included as evidence was the result of an insider selling or giving information to an outside source. These networks were not invaded by state-proxy hackers, but accessed by employees with nefarious goals.
8. The U.S. Cyber Consequences Unit is a nonprofit organization that works on cybersecurity issues primarily as a government contractor (it would seem). See http://www.usccu.us.

## References


Baumann, N. 2013. You'll never guess where this FBI agent left a secret interrogation manual. *Mother Jones*, December 20. http://www.motherjones.com/politics/2013/12/fbi-copyrighted-interrogation-manual-unredacted-secrets (accessed March 17, 2016).

Beers, R. 2013. Written testimony of DHS Acting Secretary Rand Beers for a senate committee on homeland security and governmental affairs hearing titled 'Threats to the Homeland.' November 13. https://www.dhs.gov/news/2013/11/14/written-testimony-dhs-acting-secretary-rand-beers-senate-committee-homeland-security (accessed March 17, 2016).

Bettig, R. V. 1996. *Copyrighting culture: The political economy of intellectual property*. Boulder, CO: Westview Press.

Blair, D. C., and J. M. Huntsman, eds. 2013. *The report of the commission on the theft of American intellectual property*. Seattle, WA: National Bureau of Asian Research. http://ipcommission.org/report/IP_Commission_Report_052213.pdf (accessed March 17, 2016).

Boldrin, M., and D. K. Levine. 2008. *Against intellectual monopoly*. Cambridge, UK: Cambridge University Press.

Bollier, D. 2002. *Silent theft: The private plunder of our common wealth*. New York, NY: Routledge.

Boyle, J. 1996. *Shamans, software, and spleens: Law and the construction of the information society*. Cambridge, MA: Harvard University Press.

Boyle, J. 2003. The second enclosure movement and the construction of the public domain. *Law and Contemporary Problems* 66 (1):33–74.

Brito, J., and T. Watkins. 2011. The cybersecurity–industrial complex. *Reason* 43 (4):28–35.

Browning, C. S., and M. McDonald. 2011. The future of critical security studies: Ethics and the politics of security. *European Journal of International Relations* 19 (2):235–55.

Buzan, B., O. Wver, J. De Wilde, et al. 1997. *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner Publishers.

Campbell, D. 1998. *Writing security: United States Foreign policy and the politics of identity*, rev. ed. Minneapolis, MN: University of Minnesota.

Cartalucci, T. 2013. In memory of Aaron Swartz: Here are 14 ways to fight back against the 'intellectual property' racket. Films for Action. http://www.filmsforaction.org/takeaction/in_memory_of_aaron_swartz_here_are_14_ways_to_fight_back_against_the_intellectual_property_racket (accessed March 16, 2015).

Carter, A. 2015. *The DOD cyber strategy*. Washington, DC: Department of Defense. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed March 27, 2016).

Cavelty, M. D. 2007. *Cyber-security and threat politics: US efforts to secure the information age*. London, UK: Routledge.

Clarke, R. A., and R. K. Knake. 2010. *Cyber war: The next threat to national security and what to do about it*. New York, NY: Ecco.

Clarke, R. A., M. J. Morell, G. R. Stone, C. R. Sunstein, and P. Swire. 2013. *Liberty and security in a changing world: Report and recommendations of The President's Review Group on Intelligence and Communications Technologies*. Washington, DC: The White House. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed March 17, 2016).

Correa, C. 2000. *Intellectual property rights, the WTO, and developing countries: The TRIPS agreement and policy options*. New York, NY: Zed Books and Third World Network.

Daniel, L. 2012. DOD needs industry's help to catch cyber attacks, commander says. U.S. Department of Defense. March 27. http://archive.defense.gov/news/newsarticle.aspx?id=67713 (accessed March 27, 2016).

Defense Security Service. 2012. Targeting U.S. technologies: A trend analysis of reporting from defense industry, 2012. http://www.dss.mil/documents/ci/2012-unclass-trends.pdf. (accessed March 27, 2016).

Deibert, R. J. 2013. *Black code: Inside the battle for cyberspace*. Plattsburgh, NY: Signal.

Deibert, R., and R. Rohozinski. 2010. Liberation vs. control: The future of cyberspace. *Journal of Democracy* 21 (4):43–57.

Denning, D. E. 1998. *Information warfare and security*. New York, NY: Addison-Wesley.

Doctorow, C. 2008. *Content: Selected essays on technology, creativity, copyright, and the future of the future*. San Francisco, CA: Tachyon Publications.

Donahue, T., and D. Hirschmann. 2008. Intellectual property: Creating jobs, saving lives, improving the world. Global Intellectual Property Center. [On file with author].

Drahos, P. 2003. *Information feudalism: Who owns the knowledge economy?* New York, NY: New Press.

Eun, Y.-S., and J. S. Abmann. 2014. Cyberwar: Taking stock of security and warfare in the digital age. *International Studies Perspectives*. Advance online publication: 1–18.

Farwell, J. P., and R. Rohozinski. 2012. The new reality of cyber war. *Survival* 54 (4):107–20.

Federal Bureau of Investigation. 2013. Federal Bureau of Investigation Pro IP Act annual report. 2012. Department of Justice. http://www.justice.gov/dag/iptaskforce/proipact/fbi-pro-ip-rpt2012.pdf (accessed March 17, 2016).

Gartzke, E. 2013. The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security* 38 (2):41–73.

Gjelten, T. 2013. Is all the talk about cyberwarfare just hype? 2013. *NPR.org*. http://www.npr.org/2013/03/15/174352914/is-all-the-talk-about-cyberwarfare-just-hype (accessed March 27, 2016).

Halbert, D. 1997. Intellectual property piracy: The narrative construction of deviance. *International Journal for the Semiotics of Law* 10 (1):55–78.

Halbert, D. 2005. *Resisting intellectual property*. London, UK: Routledge.

Hansen, L., and H. Nissenbaum. 2009. Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly* 53:1155–75.

Hemmungs Wirtén, E. 2004. *No trespassing: Authorship, intellectual property rights, and the boundaries of globalization*. Toronto, ON, Canada: University of Toronto Press.

Hollis, D. B. 2011. An E-SOS for cyberspace. *Harvard International Law Journal* 52 (2):373–432.

Hurwitz, R. 2015. A call to cybernorms. Harvard, MIT and University of Toronto, American Bar Association Cybersecurity Legal Task Force. https://www.americanbar.org/content/dam/aba/uncategorized/GAO/2015apr14_acalltocybernorms.authcheckdam.pdf (accessed March 17, 2016).

Lachow, I. 2013. *Active cyber defense: A framework for policymakers*. Washington DC: Center for a New American Security. http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf (accessed March 27, 2016).

Langevin, J., M. McCaul, S. Charney, and H. Raduege. 2008. *Securing cyberspace for the 44th presidency: A report of the CSIS commission on cybersecurity for the 44th presidency*. Washington DC: Center for Strategic and International Studies.

Larsson, S. 2013. Sociology of law in a digital society—A tweet from global Bukowina, *Societas/Communitas* 15 (1):281–95.

Lessig, L. 2002. *The future of ideas: The fate of the commons in a connected world*. New York, NY: Vintage.

Lessig, L. 2005. *Free culture: The nature and future of creativity*. New York, NY: Penguin (Non-Classics).

Lessig, L. 2006. *Code: And other laws of cyberspace, version 2.0*. New York, NY: Basic Books.

Lessig, L. 2013. Prosecutor as bully. *Huffington Post*, January 14. http://www.huffingtonpost.com/lawrence-lessig/aaron-swartz-suicide_b_2467079.html (accessed March 17, 2016).

Libicki, M. C. 2007. *Conquest in cyberspace: National security and information warfare*. New York, NY: Cambridge University Press.

Lindsay, J. R. 2015. The impact of China on cybersecurity: Fiction and friction. *International Security* 39 (3):7–47.

Mandiant Intelligence Center. 2013. APT1: Exposing one of China's cyber espionage units. Mandiant Intelligence Center. http://intelreport.mandiant.com (accessed March 17, 2016).

Manjikian, M. M. 2010. From global village to virtual battlespace: The colonizing of the Internet and the extension of Realpolitik. *International Studies Quarterly* 54 (2):381–401.

May, C. 2000. *A global political economy of intellectual property rights: The new enclosures?* London, UK: Routledge.

May, C., and S. K. Sell. 2006. *Intellectual property rights: A critical history*. Ipolitics. Boulder, CO: Lynne Rienners Publishers.

McGraw, G. 2013. Cyber war is inevitable (unless we build security in). *Journal of Strategic Studies* 36 (1):109–19.

McLeod, K. 2007. *Freedom of expression®: Resistance and repression in the age of intellectual property*. Minneapolis, MN: University of Minnesota Press.

Mertha, A. 2005. *The politics of piracy: Intellectual property in contemporary China*. Ithaca, NY: Cornell University Press.

Michaels, J. 2013. Pentagon expands cyber-attack capabilities. *USA Today*. April 21. http://www.usatoday.com/story/news/nation/2013/04/21/pentagon-expanding-offensive-cyber-capabilities/2085135 (accessed March 17, 2016).

Mueller, M., J. Mathiason, and H. Klein. 2007. The internet and global governance: Principles and norms for a new regime. *Global Governance: A Review of Multilateralism and International Organizations* 13 (2):237–54.

Neigel, C. 2000. Piracy in Russia and China: A different U.S. reaction. *Law and Contemporary Problems* 63:179–99.

Obama, B. 2011. *International strategy for cyberspace: Prosperity, security, and openness in a networked world*. Washington, DC: The White House.

Obama, B. 2013. Executive order—Improving critical infrastructure cybersecurity. The White House, February 12. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed March 17, 2016).

Office of the National Counterintelligence Executive. 2011. Foreign spies stealing US economic secrets in cyberspace: Report to Congress on foreign economic collection and industrial espionage, 2009–2011. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed March 17, 2016).

Ophardt, J. A. 2010. Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. *Duke Law & Technology Review* 2010 (3):i–xxvii.

Peñalver, E., and S. Katyal. 2010. *Property outlaws: How squatters, pirates, and protesters improve the law of ownership*. New Haven, CT: Yale University Press.

Pooley, J. 2013. Trade secrets: The other IP right. *WIPO Magazine*, June. http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html (accessed March 17, 2016).

Reagan, R. 1984. National security decision directive number 145 national policy on telecommunications and automated information systems security. Federation of American Scientists: Presidential Directives and Executive Orders, September 17. http://fas.org/irp/offdocs/nsdd145.htm (accessed March 17, 2016).

Reilly, R. J. 2013a. Aaron swartz prosecutors weighed 'guerilla' manifesto, justice official tells congressional committee. *Huffington Post*, February 22. http://www.huffingtonpost.com/2013/02/22/aaron-swartz-prosecutors_n_2735675.html (accessed March 17, 2016).

Reilly, R. J. 2013b. Eric Holder: Aaron Swartz case 'A good use of prosecutorial discretion.' *Huffington Post*, March 6. http://www.huffingtonpost.com/2013/03/06/eric-holder-aaron-swartz_n_2819161.html (accessed March 17, 2016).

Rid, T. 2012. Cyber war will not take place. *Journal of Strategic Studies* 35 (1):5–32.

Rid, T. 2013. *Cyber war will not take place*. New York, NY: Oxford University Press.

Riley, M., and J. Walcott. 2011. China-based hacking of 760 companies shows cyber cold war. *Bloomberg*, December 14. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html (accessed March 17, 2016).

Schmidt, M. S., and D. E. Sanger. 2014. 5 in China army face U.S. charges of cyberattacks. *New York Times*, May 19. http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html (accessed March 17, 2016).

Schmitt, M. N., ed. 2013. *Tallinn manual on the international law applicable to cyber warfare*. Reprint. Cambridge, UK: Cambridge University Press.

Schulz, G. W. 2013. Government secrecy orders on patents have stifled more than 5,000 inventions. *Wired*, April 16. http://www.wired.com/2013/04/gov-secrecy-orders-on-patents (accessed March 17, 2016).

Sharma, A. 2010. Cyber wars: A paradigm shift from means to ends. *Strategic Analysis* 34 (1):62–73.

Singer, P. W., and A. Friedman. 2014. *Cybersecurity and cyberwar: What everyone needs to know*. New York, NY: Oxford University Press.

Snowden, E. 2014. Here's how we take back the Internet. http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet (accessed March 27, 2016).

Stallman, R. M. 2006. Don't let 'intellectual property' twist your ethos. GNU Operating System, June 9. http://www.gnu.org/philosophy/no-ip-ethos.html (accessed March 17, 2016).

Stallman, R. M., L. Lessig, and J. Gay. 2002. *Free software, free society: Selected essays of Richard M. Stallman*. Boston, MA: Free Software Foundation.

Stevens, T. 2012. A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy* 33 (1):148–70.

Stone, J. 2013. Cyber war will take place! *Journal of Strategic Studies* 36 (1):101–8.

Svensson, M., and S. Larsson. 2012. Intellectual property law compliance in Europe: Illegal filesharing and the role of social norms. *New Media & Society* 14(7):1147–1163.

The White House. 2003. *The national strategy to secure cyberspace*. Washington DC: The White House. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed March 17, 2016).

The White House. 2009. Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure. http://www.whitehouse.gov/assets/documents/Cyber-space_Policy_Review_final.pdf (accessed March 17, 2016).

Treverton, G., C. Matthies, K. J. Cunningham, J. Goulka, G. Ridgeway, and A. Wong. 2009. *Film piracy, organized crime and terrorism*. Santa Monica, CA: Safety and Justice Program and the Global Risk and Security Center. RAND Corporation. www.rand.org/pubs/monographs/2009/RAND_MG742.pdf (accessed March 27, 2016).

Uzal, R., N. C. Debnath, D. Riesco, and G. Montejano. 2014. Trust in cyberspace: New information security paradigm. In *Managing trust in cyberspace*, ed. S. M. Thampi, B. Bhargava, and P. K. Atrey, 405–18. Boca Raton, FL: Taylor & Francis.

Vaidhyanathan, S. 2001. *Copyrights and copywrongs: The rise of intellectual property and how it threatens creativity*. New York, NY: New York University Press.

van Munster, R. 2005. *Logics of security: The Copenhagen School, risk management and the war on terror*. Political Science Publications. Odense, Denmark: Syddansk Universitet. http://static.sdu.dk/mediafiles/Files/Om_SDU/Institutter/Statskundskab/Skriftserie/05RVM10.pdf (accessed March 17, 2016).

Ventre, D., ed. 2011. *Cyberwar and information warfare*. Hoboken, NJ: Wiley-ISTE.

Williams, M. C. 2003. Words, images, enemies: Securitization and international politics. *International Studies Quarterly* 47:511–31.

Yu, P. 2005. U.S.-China trade: Opportunities and challenges—Still dissatisfied after all these years: Intellectual property, post-WTO China, and the avoidable cycle of futility. *Georgia Journal of International and Comparative Law* 34 (1):143.

Yu, P. 2006. From pirates to partners (Episode II): Protecting intellectual property in post-WTO China. *American University Law Review* 55 (4):901.