What Should be the Role and Responsibility of the Government in Defending Private and Commercial Digital Intellectual Property?

Ron Shachar

The rapid development of cyberspace has led to a growing threat of criminally motivated cybertheft of intellectual property in general, and of commercial and private digital trade secrets in particular. This kind of cybercrime could have a critical impact on the international macro-economic system, including potential massive loss of tax revenue and drop in GDP. While most countries have strategic cyber defense doctrines to protect their physical critical infrastructures against politically motivated cyber warfare, they still lack suitable doctrines, legislation, and means of protecting digital intellectual property against criminally motivated cybercrimes. Furthermore, the outdated approach of consequential penalties against cybercrimes is irrelevant, as cyberspace makes it difficult to detect the intellectual property theft in real time. In this article, we will analyze whether the macro-economic implications of the growing cybertheft trends will help render the commercial and private digital intellectual property as critical infrastructure that should be proactively protected by governments against cybertheft.

Keywords: digital intellectual property, cybertheft, critical infrastructure, governmental responsibility, cybercrime, CNE, proactive protection, cyber defense doctrines, macro-economic implications

Ron Shachar is a private Cyber Strategic Consultant, who has served in the IDF as head of the Cyber-Defense Strategic Planning Section and as assistant to the Cyber-Defense Unit's Director.

Introduction

> From now on, our digital infrastructure – the networks and computers we depend on every day – will be treated as they should be: as a strategic national asset.[1]
>
> We are going to aggressively protect our intellectual property. 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.[2]
>
> President Barack Obama

Commercial and private digital intellectual property in general and trade secrets in particular currently are regarded as important components of the economies of modern countries. Concurrently, cyberspace is rapidly evolving to become a source of both great opportunities and threats through cyber warfare and cybercrime.[3] Some of the criminally motivated cyber threats are aimed directly at stealing commercial and private intellectual property, which could cause loss of massive tax revenue that diminish a country's economic income and GDP (Gross Domestic Product), and could have a severe impact on the international macro-economic systems.[4] While most countries have strategic cyber defense doctrines and statutes for protecting their physical critical infrastructures against politically motivated cyberattacks, they have ignored the need to protect digital intellectual property in cyberspace against criminally motivated campaigns.

The article examines why governments should treat commercial and private intellectual property in general and digital trade secrets in particular as national critical infrastructure, which deserve appropriate governmental proactive protection. We will ask whether the macro-economic implications might help to define the commercial and private digital intellectual property as critical infrastructures that should be protected against cybertheft. Although the scope here neither includes specific measures nor suggests that the governmental defense of private intellectual property should be equivalent to that of the physical critical infrastructure in cyberspace, a general framework for a better balance between the two is recommended.

Definition and Scope of Physical Critical Infrastructures

Cyberattacks are carried out through hacking, mostly from outside the network in order to retain some or full control over the network.[5] That control is used for two purposes: computer network attack (CNA) or computer network exploitation (CNE).[6] Cyberattacks also seek to undermine the computerized network for criminal, political or national security purposes.[7] Governmental agencies, competitive corporations or individuals all might have possible motivations to engage in cybertheft of digital intellectual property.

Governments have a responsibility of providing their people and national assets with protection and security.[8] The degree of fulfilling that responsibility, however, varies between countries in accordance with the particular regime. According to James A. Lewis and Katrina Timlin of the Center for Strategic and International Studies in Washington DC, as the Internet becomes a modern global infrastructure for international commercial businesses and governmental activity, security of cyberspace has become both a national and international concern.[9]

According to Dr. Kristin M. Lord and Travis Sharp, the number of cyberattacks with criminal and political motivations is growing rapidly. There are an estimated 1.8 billion attacks per month with various levels of sophistication solely targeting the US Congress and American federal agencies.[10] Eric Sterner of the American Department of Defense stipulates that the number of cyberattacks is far greater when one includes international attacks on foreign governments and private sectors.[11] Professor Eric Talbot Jensen estimates that thousands of companies around the world are currently under cyberattack, and their intellectual property, specifically their trade secrets, is being compromised.[12] In many cases, the private and commercial companies will be unaware of the attack unless the government and its agencies inform them of the attack.[13] By the time they know about the attack, it is already too late as the company's data and intellectual property have already been stolen.[14]

Of all the possible cyberattacks, the CNE type, which in the private sector manifests mostly as intellectual property theft, is the most troubling one. According to Martin C. Libicki, the CNE cyberattack is of great concern mainly because it focuses on stealing digital data and secrets while operating under the owner's radar and without being exposed, as these methods are difficult to detect.[15] Consequently, the intellectual property theft and

CNE attacks are the greatest threat to keeping and maintaining private and commercial intellectual property as secrets.

The rapid growth in cyberattacks in the international arena and their threat to global security and economic systems have evolved into ongoing cyber warfare and cybercrime, which include both trained military units motivated for political reasons and expert criminals propelled by criminal and commercial interests.[16] The increase in cyberattacks has caused governments from all around the world to establish designated agencies and cyber defense doctrines in order to deal with cyberspace threats. In the United States, the Cyber Command Agency is responsible for removing any politically motivated threats directed at military and critical cyber infrastructures, while other agencies, such as the FBI, deal with criminally motivated cyber threats.[17] This is a result of the growing reliance on networked information systems that control critical infrastructures and communications systems, which are essential to modern life.[18]

In most western countries, the evolving cyber responsibility of the government has focused on defending mainly national interests and infrastructure, while overlooking the need to defend private and commercial intellectual property. France[19] and Germany,[20] have highlighted the cyber threats against national critical infrastructure as a strategic factor prioritized within their defense doctrines. In the United Kingdom, the focus is mainly on governmental assets, activities, national organizations, and critical infrastructure such as the financial system.[21] In Israel, the police is responsible for cybercrime, even though the National Cyber Bureau in the Prime Minister's Office, which is responsible for protecting the state's critical infrastructure, has many more resources and government attention.[22]

Given the similar focus of the various countries, there is a broad consensus to prioritize the physical protection of national critical infrastructures in cyberspace. Some notorious cyberattacks of national critical infrastructures in recent years raised awareness of these sorts of attacks, and may have contributed to this consensus. Following the 2007 massive cyberattack on Estonia[23] and the 2010 Stuxnet attack on the Iranian nuclear program,[24] most countries have prioritized their cyber defense doctrines around the government's physical protection of critical infrastructures. According to Bruce Berkowitz, critical infrastructures and key assets are vital components; if they are cyberattacked, the country under attack will be brought to its knees.[25] As a result of the technological evolvement and the growing dependence of governmental and military processes on cyberspace, the

definition of critical infrastructures has expanded. Information systems and digital intellectual property are so vital to governments, civilian society, and modern militaries that they could become the main targets in war.[26] Hence, the definition of "critical infrastructure" needs to be updated to include these digital core components.[27]

Cyber warfare and its direct threat to the stability and vitality of nations has led the international community to establish national cyber defense doctrines. These strategic doctrines have tackled the politically motivated threats through physical protection of critical infrastructures. These defense doctrines, however, are insufficient for criminally motivated intellectual property theft and CNE threats to private and commercial assets. This current situation raises the question whether the macro-economic implications of the increase in cybertheft should motivate governments to consider commercial and private digital intellectual property as part of the critical infrastructure that deserves to be protected proactively against criminally and politically motivated cybertheft.

Private and Commercial Digital Intellectual Property as National Critical Infrastructure

Even though definitions might differ between countries, three criteria must be met in order for intellectual property to legally qualify as a trade secret. First, the data must give a competitive advantage when kept as a secret. Second, it must actually be kept as a secret. The secrecy criterion is an absolute one, as long as the data and information cannot be taken or extracted easily from the published product. Third, the data must be protected by a reasonable secrecy defense mechanism,[28] (including cyber defense technologies) to keep away any intruders. Some courts recognize also a fourth criterion of liability, as they demand that the secret information be continuously used in the company's business.

As mentioned earlier, many companies do not know that their data has been stolen through cyberspace and when they do find out they are often reluctant to report the loss, as they fear the potential commercial damage to their reputation.[29] Cybertheft of commercial and private intellectual property might be politically motivated − known as economic espionage (state-driven)[30] − or criminally motivated to gain private or commercial market advantage, known as industrial espionage.[31] Regardless of the initial motivations or purposes, the potential macro-economic implications for the company are vast and destructive. Companies that have been robbed

of their intellectual property use different methods to estimate their financial losses. Some companies base their estimations on the actual costs of developing the stolen secret data, while others project the loss of future gross income.[32]

In addition to the damages inflicted upon an individual company, the question arises whether the theft of individual trade secrets can have a macro-economic impact on the nation's resilience. The cybertheft of digital intellectual property damages the ability of the national financial sector to generate new revenues and jobs or develop and research new innovations,[33] causing loss of tax revenue that diminishes the country's economic income and GDP (Gross Domestic Product).[34] Consequently, a vast and large-scale cybertheft of commercial and private intellectual properties translates into serious macro-economic loss, estimated in the billions and reflected in a drop in the Gross National Product.[35] For example, an elaborate and orchestrated cybertheft of private and commercial digital trade secrets, regardless of the actual motive of the attack, might result in the sudden bankruptcy of a country as a result of a loss of massive tax revenue and income. Economic analysis, depending on the various calculation methods, estimates that the losses caused by cybertheft of trade secrets range from $2 billion to $400 billion or more per year in the United States alone.[36]

Thus, the initial motivation for the cybertheft, whether criminal or political, is insignificant when considering the cyber defense approaches as there is no connection between the purpose of the attack and the destructive macro-economic implications and the holistic preventive cyber defense solutions (technological and doctrinal). Either way, the economic impact of cybertheft on national resilience is a major one.

In the last century, the pace of innovation, and research and development (R&D) in the private and commercial sectors increased the growth of trade secrets and the number of patents issued in the United States by 40.6 percent, showcasing the powerful role of trade secrets in the global economy.[37] According to Technet, a US national coalition of CEOs in the high-tech sector, more than six million jobs and more than a third of the fifteen-trillion dollar US economy is based on innovation and consequently, on trade secrets and intellectual property.[38] General Keith Alexander, former director of the US National Security Agency and Cyber Command, has estimated the losses to the American GDP at about $250 billion a year as a result of cybertheft of trade secrets, calling it "the greatest transfer of wealth in history."[39] An example is the 2007 cybertheft of Lockheed-Martin's F-35

stealth fighter program, allegedly by a Chinese company, which had been working on a similar aircraft at the time (the J20).[40] Although this cybertheft was politically motivated, the economic impact is the same.

A good understanding of the macro-economic value of the trade secrets – and accordingly, the potential national loss of income – can be obtained by reviewing the private and commercial sector's investments in R&D. Although there are a lot of valuable and important trade secrets not related to R&D (for example, sales figures, client lists, marketing strategies, and so forth), R&D represents investment in cutting-edge technologies, ideas, and inventions, all critical components of many trade secrets.[41] R&D investments in the United States has surpassed 2.7 percent of the GDP, which stands at roughly $447 billion a year. Similarly, R&D investments are 2.9 percent in Germany, 2.0 percent in China, 1.8 percent in the United Kingdom, and 1.5 percent in Russia.[42] It is important to emphasize that any R&D investment generates other forms of new trade secrets (one dollar of R&D investment generates up to sixty-nine dollars over the following decade), and accordingly, the economic value of trade secrets is even greater than the R&D's figures.[43]

In a reality where the most valuable assets and infrastructures are digital, intangible, and easy to transfer over networks, cybertheft of intellectual property has taken on a new critical importance.[44] A 2001 report, representing fourteen US intelligence agencies, stated that cybertheft will become a "growing and persistent threat,"[45] as well as a concrete threat that the head of the US intelligence community ranks higher than terrorism.[46] According to a report issued by the Ponemon Institute, intellectual property theft in cyberspace has increased, with some companies experiencing more than seventy-two attacks per week.[47]

As intellectual property becomes more dominant and crucial in the modern economy, as evident from the above-mentioned statistics, its theft or damage will inflict enormous financial losses to the country that harbors it. National economies, therefore, are at tremendous economic risk should something happen to their commercial and private digital intellectual property. As stated in the US congressional report on industrial espionage, the theft of intellectual property from commercial and private companies undermines the private sector's ability to generate revenues, create new jobs, foster innovation, and lay the economic foundation for future growth and national security.[48] The growing importance of digital intellectual property to the modern economy, along with the potential destructive damage to a

nation's economy if stolen, renders cybertheft of intellectual property as extremely dangerous to a country's economic resiliency.

Consequently, governments should apply the same concerns and engage in a proactive defensive approach regarding cyberattacks of critical infrastructure of their commercial and private intellectual property. The rise in cybertheft attacks targeting digital intellectual property, along with the potential massive macro-economic losses, places the private and commercial digital intellectual property within the consensual definition of national critical infrastructures that should be protected by the state.

As the protection of commercial and private intellectual property against cybertheft is critical to corporate profitability and growth,[49] it should automatically be regarded as having national importance, as these commercial intellectual properties affect the national economy through taxes, additional indirect incomes, and the national GDP altogether. Thus, any wide-scale cybertheft of commercial intellectual properties might damage the nation's economic resiliency and cause a vast chain reaction that might surpass any possible cyberattack of an individual critical infrastructure. Consequently, governments should take responsibility for protecting private and commercial intellectual property and adopt a more involved and proactive approach towards their defense. This raises a dilemma, however; even though the digital intellectual property has macro-economic importance to the national resiliency, it is also a privately-owned entity that does not belong to the government.

National Copyright Models

Having characterized the current problem and the failure of governments to take responsibility for providing cyber protection of commercial and private intellectual property, we shall define and recommend a solution based on existing national copyrights models. Although copyrights are a specific type of intellectual property, some of the components of their protection may be relevant in defining the optimal governmental responsibility for defending the commercial and private digital intellectual property in general and trade secrets in particular.

The Anglo-American model aims at ensuring the public's benefit and welfare by providing economic incentives for the copyright creators, which increase the creation of new products.[50] Respectively, the government's proactive protection of digital intellectual property will encourage commercial entities and private individuals to continue to create new trade secrets.

Although some would say that there is not any empirical evidence that protection of intellectual property will increase their creation,[51] this claim might be more accurate in regard to copyrights in the field of arts and science. The creation of trade secrets in its essence is closely related to economic incentives, as they serve as an important factor in a country's economic growth; a proactive governmental cyber defense of trades secrets will attract new inventors by granting them economic incentives. Hence, there is a strong connection between governmental cyber protection of intellectual property and the double gain of both preventing macro-economic damages on a national scale as caused by cybertheft of commercial intellectual properties, and of encouraging the growth of new commercial intellectual property. These two consequential gains reflect the Anglo-American model, which benefits the public by producing more inventions and by strengthening the nation's economic resilience.

Complementary to the Anglo-American's model, the French model of property rights solidifies the government's role in keeping the intellectual property in the hands of its creator. According to the French model, based on the *droits d'auteur*, the creation cannot be alienated from its creator who possesses the property rights over his work.[52] This aspect of the French model gives the government the responsibility of ensuring that digital intellectual property is protected as the assets of its creator, while preventing alienation from its owners. In other words, the French model ensures that governmental protection of commercial and private digital intellectual property does not lead to the nationalization of privately-owned intellectual property nor to excessive government intervention in the private sector. It helps balance the appropriate degree of governmental cyber defense of commercial and private intellectual property. It also helps to achieve a more resilient national economic status and limits any overbearing intrusion of government in the private sector.

To conclude, the approach of the Anglo-American model will help stimulate the government's responsibility for protecting private and commercial digital intellectual property, as its national macro-economic implications serve the public's benefit. Components of the French model will ensure that the governmental intrusion into the private sector does not revoke the ownership of the protected intellectual property from its owner. This legal synthesis creates a balanced governmental proactive responsibility, without crossing the thin line between the public and the private sectors. Having synthesized the recommended governmental

cyber-defense responsibility, we shall examine how governments should execute that responsibility.

Governmental Proactive Role and Responsibility

Based on the above-mentioned principles and models, we will focus on two important components of the proposed governmental cyber responsibility to proactively protect commercial and private digital intellectual property. The first is the creation of dedicated cyber defense statutes, aimed at protecting commercial and private digital intellectual property of all sorts. Some countries have a unified comprehensive law and some use a set of laws in order to create full legal protection. For example, in the United States, two major trade secrets laws of a civil and criminal orientation have been legislated. First, the 1979 Uniform Trade Secrets Act (UTSA) provides an official definition and criteria for trade secrets, definition of their theft, and suitable consequential remedies (such as injunctive relief, economic compensation, attorney's fees, and so forth).[53] Second, since 1996, the Economic Espionage Act (EEA) has transformed the theft of trade secrets and economic espionage into federal crimes with the appropriate penalties.[54] Both statutes focus on the aftermath and consequential implications of theft of digital trade secrets, without proactively trying to prevent the act of cybertheft itself in real time. The legislation of statutes deters, to some degree, any potential cyber attackers and thieves, but alone is insufficient as a preventive countermeasure, since cyberspace provides the attackers with relative anonymity, including low risk of detection and difficulty in assigning any blame to the attackers.[55]

Hence, the second component is crafting a holistic cyber defense doctrine that strategically acknowledges the government's degree of responsibility and the consequential prioritization of protecting commercial and private digital intellectual property. These national cyber defense doctrines are not just declarative, but rather they embody national prioritization in terms of resource allocation (budgets, human resources, implementation of designated technological solutions, and so forth) aimed at protecting these vital digital assets. For example, in France, President François Hollande has issued a general national defense doctrine that addresses the threat of cybertheft. The French doctrine stresses the importance of protecting French scientific and technological assets, and preventing the theft of "French knowledge and know-how" of both public and private nature.[56] Another good example can be found in the United Kingdom's Cyber

Strategic Doctrine that stresses the importance of protecting the country's digital intellectual property, along with other national and military critical infrastructures.[57] In addition, the *Digital Britain Report* outlines the vision for digitalizing the United Kingdom, while emphasizing the importance of cyber defense as part of the national strategic vision.[58]

Even with these two suggested components – statutes and strategic doctrines aimed at prioritizing the protection of commercial and private digital intellectual property – it is still critical for the government to be proactive in order to prevent cybertheft. According to Professor Lawrence Lessig, the government's proactive responsibility for protecting commercial and private assets might be executed without the owner's consent or knowledge.[59] That sort of government activity means violating human rights and especially individual privacy. Furthermore, according to Glenn Greenwald, the growing government involvement in cyberspace will hurt the public's privacy while it will do very little to improve cybersecurity.[60]

The right solution should be a balanced one. The government should proactively protect commercial and private digital intellectual property, while limiting violations of private data and assets that are not classified as intellectual property. For example, governments could deploy cyber protection means throughout public/civil digital spaces such as by protecting public and common networks or national routers, rather than just protecting military networks from any hostile penetration. Hence, the optimal solution for protecting commercial and private intellectual property should be done through legislating the appropriate statutes and by establishing national strategic cyber defense doctrines, which together form the foundations for providing the government with the right tools and legitimacy to proactively defend crucial civil and private digital assets. In addition to governmental cyber protection, private and commercial companies should make efforts, using their own resources and investments, to prevent and detect any breaches inside their networks or any attempt of cybertheft.

Conclusion

> The new Economic Espionage Act will help us crack down on acts like software piracy and copyright infringement that cost American businesses billions of dollars in lost revenues, and it will advance our national security.[61]
>
> President Bill Clinton

A lot has changed since President Bill Clinton's words of hope of eliminating piracy and copyright infringement of trade secrets and other intellectual property. In the last twenty years, cyberspace has rapidly evolved and has given rise to strategic threats of cybertheft of commercial and private digital intellectual property. Simultaneously, commercial and private digital intellectual property in general and trade secrets in particular have become crucial and dominant factors in the contemporary economy.

The outdated approach of aftermath and consequential penalties is almost irrelevant nowadays, as cyberspace makes it difficult to detect cybertheft in real time and effectively assign its malicious motive to any individual, organization or country. Consequently, governments around the world should revise their own role and responsibility by assuming a proactive and preventive approach in their doctrines, legislation, and regulations. Governments should take some responsibility for protecting private and commercial digital intellectual property given their importance to the macro-economic systems, and their potential to cause massive economic fallout if stolen. Given the potential macro-economic losses, the significance of protecting the country's commercial and private intellectual properties through cyberspace should be seen as equivalent to the importance of protecting military and physical critical infrastructures. Using the Anglo-American model, government protection will expand economic incentives for creating new intellectual property. Furthermore, it will solidify the creator's individual right in keeping his developed intellectual property to himself, based on the French model.

Notes

1 President Barack Obama, "Remarks on Securing Our Nation's Cyber Infrastructure," *Office of the Press Secretary*, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

2 President Barack Obama, "Remarks by the President at the Export-Import Bank's Annual Conference," *Office of the Press Secretary*, March 11, 2010, http://www.whitehouse.gov/the-press-office/remarks-president-export-import-banks-annual-conference.

3 Cyberspace is a virtual medium consisting of an accumulation of networked computerized devices that are connected to the outside world (the Internet, for example). See Martin C. Libicki, *Cyber Deterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009).

4 Pamela Passman, Sanjay Subramanian, and George Prokop, *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets*

and Mitigate Potential Threats (Washington, DC: The Center for Responsible Enterprise and Trade, 2013), p. 8.

5 Libicki, *Cyber Deterrence and Cyberwar*.

6 CNA (Computer Network Attack) refers to attacking the network and its business processes by disrupting, denying or destroying the information stored in it. CNE (Computer Network Exploitation) refers to extracting the network by stealing its data. See US Department of Defense, *Dictionary of Military and Associated Terms* (Joint Education and Doctrine Division, 2014).

7 Oona A. Hathaway and Rebecca Crotoff, "The Law of Cyber-Attack," *California Law Review* 100, No. 4 (2012): 827.

8 Gareth Evans and Mohamed Shanoun, *The Responsibility to Protect: Report for the International Commission on Intervention and State Sovereignty* (Ottawa: International Development Research Centre, 2001), p.13.

9 James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington, DC: Center for Strategic and International Studies, 2011), p. 3.

10 Kristin M. Lord and Travis Sharp, *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, DC: Center for a New American Security, 2011), p. 7.

11 Eric R. Sterner, "Deterrence in Cyberspace: Yes, No, Maybe?" In *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*, ed. Robert Butterworth (Arlington, VA: George C. Marshall Institute, 2011), pp. 28-35.

12 Eric Talbot Jensen, "Cyber Warfare and Precautions Against the Effects of Attacks," *Texas Law Review* 88 (2010): 1536.

13 Kim Zetter, "Report Details Hacks Targeting Google, Others," *WIRED*, February 3, 2010, http://www.wired.com/threatlevel/2010/02/apt-hacks/.

14 Ibid.

15 Libicki, *Cyber Deterrence and Cyberwar*, p. 23.

16 Abraham R. Wagner, "Cybersecurity: From Experiment to Infrastructure," *Defense Dossier* 4 (2012): 17.

17 Lewis and Timlin, *Cybersecurity and Cyberwarfare,* p. 22.

18 The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011), p. 9.

19 Lewis and Timlin, *Cybersecurity and Cyberwarfare,* p. 11.

20 Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (Berlin: Federal Minister of the Interior, 2011).

21 UK Office of Cyber Security and UK Cyber Security Operations Centre, *Cyber Security Strategy: Safety, Security and Resilience in Cyber Space* (London, 2009), p. 9.

22 Israel's Prime Minister's Office, *Advancing National Cyber Space Capabilities-Decision Number 3611* (August 7, 2011).

23 Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review* 56 (2011): 569.

24 Thomas M. Chen, "Stuxnet, the Real Start of Cyber Warfare?" *IEEE Network* 24, no. 6 (2010): 3.
25 Bruce D. Berkowitz, "Warfare in the Information Age," In *In Athena's Camp: Preparing for Conflict in the Information Age*, eds. John Arquilla, and David Ronfeldt (Santa Monica: RAND National Security Research Division, 1997), p. 181.
26 Ibid., pp. 177, 181.
27 Myriam A. Dunn, "Securing the Information Age: The Challenges of complexity for Critical Infrastructure Protection and IR Theory," *International Relations and Security in the Digital Age* (ETH Zurich: Center for Security Studies, 2007), p. 11.
28 Robert G. Bone, "A New Look at Trade Secret Law: Doctrine in Search of Justification," *California Law Review* 86 (1998): 248-249.
29 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (2011), http://www.ncix.gov/publications/reports/fecie_all/ Foreign_Economic_Collection_2011.pdf.
30 Ibid., p. 7.
31 Ibid., p. 8.
32 Ibid., p. 2.
33 Ibid., p. 3.
34 Passman, Subramanian, and Prokop, *Economic Impact of Trade Secret Theft,* p. 8.
35 Shahar Argaman and Gabi Siboni, "Commercial and Industrial Cyber Espionage in Israel," *Military and Strategic Affairs* 6 (2014): 51, http://media.wix.com/ugd/d48d94_a62f01468dc8448ebe635f8d962c410f.pdf.
36 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets,* p. 4.
37 Passman, Subramanian, and Prokop, *Economic Impact of Trade Secret Theft,* p. 7.
38 Dennis C. Blair and Jon M. Huntsman, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (n.p.: The National Bureau of Asian Research, 2013), p. 23.
39 Carrie Lukas, "It's Time for The U.S. to Deal with Cyber-Espionage," *U.S. News*, June 4, 2013, http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy.
40 *Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People's Republic of China: Hearing on the Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology, Before the Oversight and Investigations Subcommittee of the Foreign Affairs Committee of the U.S. House of Representatives* (2011) (statement of Richard D. Fisher, Jr., Senior Fellow, International Assessment and Strategy Center, p. 5).
41 Passman, Subramanian, and Prokop, *Economic Impact of Trade Secret Theft,* p. 8.

42 Ibid.
43 Ibid.
44 Blair and Huntsman, *The IP Commission Report,* p. 43.
45 Siobhan Gorman, "China Singled Out for Cyber Spying," *Wall Street Journal*, November 4, 2011, http://allthingsd.com/20111104/china-singled-out-for-cyberspying/.
46 Argaman and Siboni, "Commercial and Industrial Cyber Espionage in Israel," 54.
47 Ponemon Institute, *Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies* (Ponemon Institute, 2011).
48 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets,* p. 3.
49 Ibid, p. A-2.
50 Neil Netanel, "Copyright Alienability Restrictions and the Enhancement of Author Autonomy: A Normative Evaluation," *Rutgers Law Journal* 24 (1993): 9.
51 Richard Watt, "An Empirical Analysis of the Economics of Copyright: How Valid are the Results of Studies in Developed Countries for Developing?" in *The Economics of Intellectual Property* (n.p.: WIPO, 2006), p. 68.
52 Netanel, "Copyright Alienability Restrictions," 15.
53 Uniform Trade Secrets Act §§ 1-12 (amended 1985).
54 The Economic Espionage Act, 18 U.S.C.§§ 1831−1839 (1996).
55 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets* p. 1.
56 President of the French Republic's Office, *French White Paper: Defense and National Security* (2013), p. 102.
57 United Kingdom's Prime Minister's Office, *Cyber Security Strategy: Safety, Security and Resilience in Cyber Space* (2009), p. 9.
58 The United Kingdom's Department of Culture, Media and Sport & the Department for Business, Innovation and Skills, *Digital Britain: Final Report* (2009), pp. 189-207.
59 Lawrence Lessig, "The Law of the Horse: What Cyber Law Might Teach," *Harvard Law Review* 113 (1999): 5.
60 Glenn Greenwald and Ewen MacAskill, "Obama Orders US to Draw Up Overseas Target List for Cyber-attacks," *Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.
61 President Bill Clinton, "Statement on Signing the Economic Espionage Act of 1996," October 11, 1996, in Weekly Compilation of Presidential Documents, 32, no. 41 (October 14, 1996), http://www.gpo.gov/fdsys/pkg/WCPD-1996-10-14/html/WCPD-1996-10-14-Pg2040.htm.