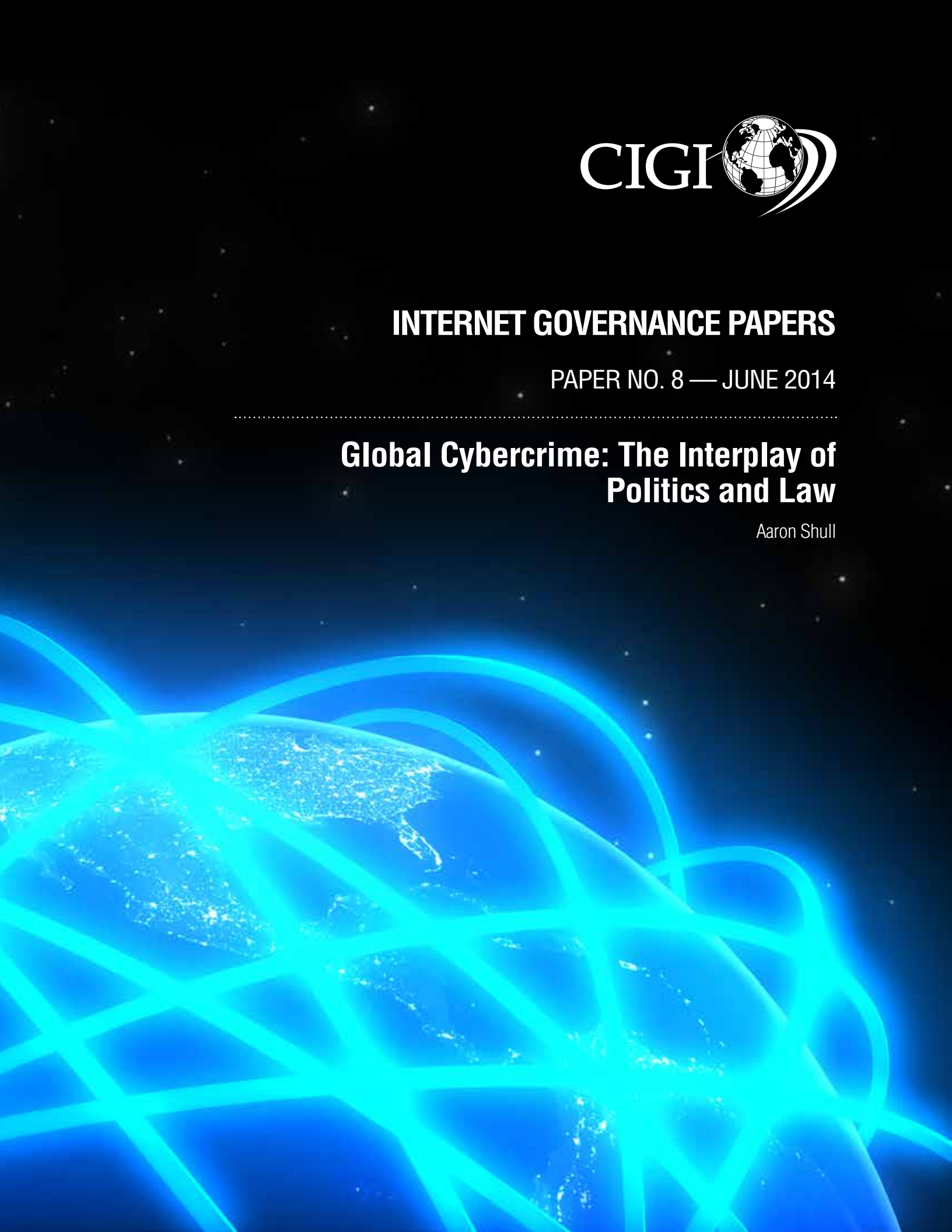

CIGI

INTERNET GOVERNANCE PAPERS

PAPER NO. 8 — JUNE 2014

Global Cybercrime: The Interplay of Politics and Law

Aaron Shull

INTERNET GOVERNANCE PAPERS
PAPER NO. 8 — JUNE 2014

Global Cybercrime: The Interplay of Politics and Law

Aaron Shull

ACKNOWLEDGEMENT

CIGI gratefully acknowledges the support of the Copyright Collective of Canada.

CIGI

CONTENTS

ABOUT ORGANIZED CHAOS: REIMAGINING THE INTERNET PROJECT

Historically, Internet governance has been accomplished *en passant*. It has emerged largely from the actions of computer scientists and engineers, in interaction with domestic legal and regulatory systems. Beginning at least with the 2003–2005 World Summit on the Information Society process, however, there has been an explicit rule-making agenda at the international level. This strategic agenda is increasingly driven by a coalition of states — including Russia, China and the Arab states — that is organized and has a clear, more state-controlled and monetary vision for the Internet. Advanced industrial democracies and other states committed to existing multi-stakeholder mechanisms have a different view — they regard Internet governance as important, but generally lack coherent strategies for Internet governance — especially at the international level. Given the Internet's constant evolution and its economic, political and social importance as a public good, this situation is clearly untenable.

A coherent strategy is needed to ensure that difficult trade-offs between competing interests, as well as between distinct public values, are managed in a consistent, transparent and accountable manner that accurately reflects public priorities. Guided by these considerations, CIGI researchers believe they can play a constructive role in creating a strategy for states committed to multi-stakeholder models of Internet governance.

In aiming to develop this strategy, the project members will consider what kind of Internet the world wants in 2020, and will lay the analytical groundwork for future Internet governance discussions, most notably the upcoming decennial review of the World Summit on the Information Society. This project was launched in 2012. The Internet Governance Paper Series will result in the publication of a book titled *Organized Chaos: Reimagining the Internet* in 2014.

ABOUT THE AUTHOR

Aaron Shull is a research fellow and CIGI's counsel and corporate secretary. An expert in global security issues and international law, he contributes to research activity under CIGI's Global Security & Politics Program and International Law Research Program, and advises CIGI's senior management on a range of legal issues Called to the Bar in 2009, Aaron has practised law for a number of organizations, focusing on international, regulatory and environmental law. He has taught courses at the Faculty of Law, University of Ottawa and the Norman Paterson School of International Affairs, and was previously a staff editor for the *Columbia Journal of Transnational Law*.

EXECUTIVE SUMMARY

Examining global cybercrime as solely a legal issue misses an important facet of the problem. Understanding the applicable legal rules, both domestically and internationally, is important. However, major state actors are using concerted efforts to engage in nefarious cyber activities with the intention of advancing their economic and geostrategic interests. This attempt to advance a narrow set of economic interests through cybercrime and economic cyber espionage holds to the potential to erode the trust in the digital economy that has been a necessary condition for the success of the Internet as an economic engine for innovation and growth. By pursuing these efforts, states are prioritizing short-term interests over long-term stability and a responsibly governed, safe and secure Internet platform. This paper explores the recent unsealing of a 31-count indictment against five Chinese government officials and a significant cyber breach, perpetrated by Chinese actors against Western oil, energy and petrochemical companies. The paper concludes by noting that increased cooperation among governments is necessary, but unlikely to occur as long as the discourse surrounding cybercrime remains so heavily politicized and securitized. If governments coalesced around the notion of trying to prevent the long-term degradation of trust in the online economy, they may profitably advance the dialogue away from mutual suspicion and toward mutual cooperation.

INTRODUCTION

Global cybercrime has become a modern economic plague. It has decimated corporations, increased transaction costs, undermined trust in electronic commerce and exposed the sensitive personal data of millions of Internet users. Hardly a day goes by without a front-page story addressing some new vulnerability. Earlier this year, the "Heartbleed" bug exposed a good portion of secure servers to potentially nefarious infiltration, eBay was hacked and security vulnerabilities at US retailer Target compromised the credit card data of millions of customers. At the same time that private companies struggle to address the severity of these intrusions, many governments are left in a difficult position. Seen as the natural bulwark against criminal activity, the government is charged with the responsibility for interdicting illicit enterprise. However, cybercrime is an international phenomenon and national laws do not typically extend past the border. What is lacking is a coordinated international response that matches the gravity of circumstance.

The coordination necessary at the international level is unlikely to be forthcoming in the near future. While there is an international convention aimed at combatting cybercrime, the treaty has been criticized for being regional in nature as opposed to truly global, and for being an ineffective mechanism because of its failure to attract the adherence of a number of the largest and most powerful states (Marion 2010). As the authors of other papers in this series have made clear in their contributions, there is a tremendous amount of uncertainty in the Internet governance policy space. Ronald J. Deibert noted the need for coordination at multiple levels with a wide variety of stakeholders. James A. Lewis recognized the need for different roles among the multi-stakeholder community with an explicit role for government. Keeping in line with these authors, this paper argues that global cybercrime is an area of Internet governance that calls out for increased cooperation among and between states and transnational stakeholders. The problem is that effectively interdicting acts of international cybercrime is not simply a legal challenge; it is an inherently political one as well.

This paper is an attempt to analyze, from domestic and international perspectives the stark legal challenges created by the ever-intensifying glut of cybercrime committed across national borders. The point here is not to be alarmist about the increase in crime committed over the Internet, or about the amount of money, intellectual property or confidential information being stolen. Rather, the purpose is to show, from a legal perspective, just how difficult it is to successfully bring an international cybercriminal to justice, while shedding some additional light on the interplay between global politics and law in this area of Internet governance.

In order to accomplish this, these systemic tensions will be explored using the relationship between the Chinese and US governments as a case for analysis. In particular, this paper will explore the recent unsealing of a 31-count indictment against five Chinese government officials, charging them with various cyber-related offences in the United States (Department of Justice [DoJ] 2014). The paper will also examine another high-profile example of a significant cyber breach, perpetrated by Chinese actors against Western oil, energy and petrochemical companies. This attack, dubbed the "Night Dragon," led not only to intrusion into US companies, but was detected in the Americas, Europe, Asia, the Middle East and North Africa.[1] These examples will be used to demonstrate the practical difficulties surrounding the investigation and prosecution of international cybercriminals, and to provide support for the argument that the success of enforcement efforts against international cybercriminals is more contingent on political and strategic concerns than on legal ones.

While the examples employed focus on the relationship between the United States and China, this should not be taken to mean that the concerns set out are unique to the relationship between these two governments. Rather, the reality is that cybercrime is truly global, touching governments, companies and individuals all around the world. The relationship between the United States and China is simply one example that can be used to demonstrate the legal, political and technical challenges implicated in this policy arena.

The second part of this paper will provide additional background on the recent indictment of various Chinese officials by the US Attorney General and the Night Dragon attack. In this context, the third part focuses on the specific legal problems faced when attempting to prosecute cybercrime internationally, especially in cases where the domestic laws within the offending state are vague, the extraterritorial application of the victim state's law is unclear and other international legal remedies are ineffective. The fourth part deals with the applicable provisions of domestic Chinese cyber law and the politicized nature of US-Chinese relations in this area. It will be argued that while China does have certain "laws on the books" that could potentially apply to the types of attacks alleged to have been committed both in the indictment and during the Night Dragon cyber raids, the substance of those laws and their enforcement is grossly inadequate. This problem is unlikely to be remedied given China's strategic interest in actively encouraging economic espionage of this kind. The fifth part examines the existing international legal regime that would govern potential cooperation between the United States and China, and concludes that given the ad hoc nature of any international efforts to combat this type of cybercrime, politics will likely undermine appropriate levels of legal evolution and enforcement. As it stands, the two countries have significantly divergent geostrategic interests, a fact that is likely to undermine the prospect of

1 See www.mcafee.com/us/about/night-dragon.aspx?cid=WBB009.

meaningful legal cooperation in this area — at least in the near term.

CONTEMPORARY CYBERCRIME: NIGHT DRAGON AND THE US INDICTMENTS

The Indictments and US-China Relations

Tensions resulting from cybercrime and cyber espionage have been high in the relationship between China and the United States. Both governments seem suspicious, but have usually remained circumspect in their public statements regarding the other's activities. On both sides, however, both the rhetoric and the responses have been ratcheting up.

In its annual report to Congress, the Office of the Secretary of Defense (2013) accused the Chinese government of employing a concerted government-led strategy to use cyber exploits to advance strategic interests and to steal intellectual property. These exploits, the report contends, can be used to benefit China's defence industry, high technology industries and the broader interests of Chinese policy makers (ibid., 36).

China has also claimed to be victim to cyber espionage, particularly following the revelations made by former NSA contractor Edward Snowden. Prior to the NSA leaks, bilateral meetings between the two nations led to the creation of a joint China-US Cyber Working Group, in order to ease strain and foster mutual cooperation (Jones 2013), and address the long-standing issue of cyber espionage between the United States and China (Schmidt and Sanger 2014). The working group continued to meet following the disclosures, with the goal of "speed[ing] up action to prevent hacking attacks" (BBC News 2013). In this respect, both parties have claimed to be victims of cyber espionage, making enhanced cooperation appear to be an important objective.

Despite these efforts to encourage cooperation on the issue of cyber security between the United States and China, on May 1, 2014, the United States filed an indictment charging five Chinese military officials for cyber espionage directed at American corporations in the United States' nuclear power, metals and solar products industries (DoJ 2014). The victims were five corporations (Westinghouse Electric Company, US subsidiaries of SolarWorld AG, United States Steel Corporation, Allegheny Technologies Inc. and Alcoa Inc.) and one workers' union (the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union).

The five individuals were charged with 31 counts, including computer hacking, economic espionage, conspiring to commit fraud and abuse, trade secret theft and aggravated identity theft. It is alleged that the hackers stole trade secrets as well as "sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity" (ibid.)

The Chinese government has vehemently denied the accusations against the five military hackers, demanding they be withdrawn and saying the indictment "grossly violates the basic norms governing international relations and jeopardizes China-U.S. cooperation" (Schmidt and Sanger 2014). It has responded with a government agency report claiming "unscrupulous US cyber-spying" citing previous media reports concerning Edward Snowden's NSA leaks, as well as a subsequent investigation, which "confirmed the existence of snooping activities directed against China" (Associated Press 2014). In addition to denying the US claims, the Chinese government is suspending its involvement in the joint China-US Cyber Working Group.

Nevertheless, it is uncertain how effective this indictment will be. Given the lack of extradition laws

between the United States and China, and the fierce denial of accusations by Beijing, it is unlikely that the five individuals named in the indictment will actually see the inside of a US courtroom.

The Night Dragon Attacks

In 2011, McAfee, one of the largest global Internet security companies, released a startling report indicating that starting in November 2009, coordinated "covert and targeted cyberattacks" were conducted against Western oil, energy and petrochemical companies (McAfee Foundstone Professional Services and McAfee Labs 2011). The attacks were multipronged, involving more than one exploit modality, using "social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of remote administration tools (RATs) in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations" (ibid., 3). What makes these particular attacks so devious is that "attackers using several locations in China have leveraged C&C [command-and-control] servers on purchase hosted services in the United States and compromised servers in the Netherlands to wage attacks against global oil, gas, and petrochemical companies, as well as individuals and executives in the United States to acquire proprietary and highly confidential information" (ibid., 4).

While advanced computer experts might refer to the Night Dragon attack modalities as relatively unsophisticated, the reality is that the network security breaches were methodical and, more critically, they were successful — compromising the networks of multinational energy enterprises (ibid., 7). Moreover, clandestine cyber infiltrations like the Night Dragon attacks are an increasing phenomenon, with significant financial implications for the victims. Intellectual property, negotiating positions and confidential financial and corporate information are all at risk of exposure. Government agencies and military or defense contractors are no longer the sole targets of these types of concerted cyber attacks. Rather, multinational corporate and commercial enterprises now find themselves increasingly under siege. The fact is that while the "Night Dragon attacks focused specifically on the energy sector, the tools and techniques of this kind can be highly successful when targeting any industry" (ibid., 13). These attacks are just one example of an increasing number of cyber attacks directed at companies. This highlights the importance of determining what legal tools are available to domestic law enforcement to investigate, interdict and prosecute cybercriminals who are, as in the case of the Night Dragon attacks, physically present in another jurisdiction.

THE APPLICATION OF DOMESTIC LAW TO INTERNATIONAL CYBERCRIME

Cybercrime is a global phenomenon, touching every corner of the earth. A global survey is outside the scope of this paper; however, the legal regime within the United States has been selected for further analysis. The United States is a major target for these types of acts, and is also a primary player in the political sphere that is driving the evolution of cooperation (or lack thereof) around international cybercrime.

The United States has a well-developed, robust and sophisticated legal regime that prohibits the various types of cybercrime alleged to have been committed in the indictment against the five Chinese officials and during the Night Dragon infiltration. Even with several appreciable criminal prohibitions in force, some scholars have been critical of the current regime as being outdated, underdeveloped or having insufficient extraterritorial reach (Hathaway 2012,

817). Some of these critiques may be valid; however, this paper proceeds to examine the law as it is, not as it should be. As a consequence, articulating the substance of the relevant legal rules is relatively straightforward. Moreover, while there are various legal prohibitions that could arguably be contravened by the impugned conduct, a comprehensive legal review of every conceivable contravention is outside the scope of the immediate paper; therefore, the focus will be on the charges enumerated in the indictment, the more obvious provisions of law likely contravened by the Night Dragon attacks, the investigative tools available to US authorities and the discrete legal challenges created by establishing jurisdiction.[2]

Substantive Criminal Prohibitions

The obvious starting point is the Computer Fraud and Abuse Act, section 1030 of Title 18 of the US Code (USC), which prohibits various crimes involving "protected computers."[3] The term "protected computer"[4] is a statutorily defined term, and notwithstanding the plain meaning of the words, it really has nothing to do with the either the physical or security status of the computer in question. In short, a "protected computer" is a computer that is used in, or affects, interstate or foreign commerce, or a computer that is used by the federal government or a financial institution. The relevant portion of section 1030(e)(2), which defines protected computer, states that the definition covers computers:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is *used in or affecting interstate or foreign commerce or communication*.... [emphasis added]

Therefore, the broadly applicable provision addressing the private industry computers affected by the Night Dragon would be the protections afforded to computers "used in" or "affecting" interstate commerce. This notion of use or affect vis-à-vis interstate or foreign commerce has, quite sensibly, been construed very broadly by US courts; in this regard, several courts have held that the fact that a computer employs an Internet connection is

2 Given the nature of the Night Dragon attacks, this paper will focus on the unlawful access provisions of 18 USC § 1030, although the activity captured in 18 USC § 1030 is certainly broader then mere unlawful access, including provision related to fraud, etc. Moreover, with respect to the criminal regime that applies to cyber-related crimes, there are numerous provisions that may be applicable depending on the circumstances. These include, but are not limited to: 18 USC § 1028 – Fraud and related activity in connection with identification documents, authentication features, and information; 18 USC § 1028A – Aggravated identity theft; 18 USC § 1029 – Fraud and related activity in connection with access devices; 18 USC § 1037 – Fraud and related activity in connection with electronic mail; 18 USC § 1343 – Fraud by wire, radio, or television; 18 USC § 1362 – [mischief in relation to] Communications lines, stations, or systems; 18 USC § 2252B – Misleading domain names on the Internet; 18 USC § 2252C – Misleading words or digital images on the Internet; 18 USC § 2425 – Use of interstate facilities to transmit information about a minor. Other relevant provisions can be found within the Economic Espionage Act (EEA) of 1996 (18 USC §§ 1831-1839). The EAA is concerned, in particular, with economic espionage and foreign efforts to acquire US trade secrets.

3 See Sofaer and Goodman (2001, 1, 25) and Sinrod and Reilly (2000, 177, 180-81).

4 18 USC § 1030(e)(2).

sufficient to meet this element.[5] Given that Night Dragon's victim systems were connected to the Internet, it seems clear that the threshold criteria has been met and the subject systems were "protected systems" for the purposes of US law. The indictment against the five Chinese officials also includes a number of counts alleging access (or attempting to access) a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain.

With respect to specifics, there is a broad-based prohibition against unlawfully accessing protected computers and obtaining information.[6] The relevant portion of the Computer Fraud and Abuse Act provides that whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains…information from any protected computer" has committed an offence under the code.[7] Under section 1030(a)(2), there is no required monetary threshold in order for the unlawful access to constitute a misdemeanour violation. This is obviously recognition of the fact that some confidentiality breaches are not easy to place a monetary value on, but still deserve federal legal protection. Although there is no monetary threshold for establishing a misdemeanour offence under section 1030(a)(2), the value of the information obtained during an intrusion can elevate the crime to a felony (DoJ, n.d., "Prosecuting Computer Crimes," 17). Establishing criminal liability for the unauthorized access of protected systems when there is little-to-no discernable monetary loss is an important first step; however, the nature of the theft of intellectual property is such that the true monetary damage may never be ascertained accurately. How, for example, does the prosecution convince a jury beyond any reasonable doubt that the value of the stolen information exceeded the required threshold to make the intrusion a felony, when the information stolen related to project-financing with regard to oil and gas field bids and operations? Or the negotiating position of a trade union?

Of course, given the wording of the section, the prosecution is also obliged to show that the accused actually "obtained information." Thankfully, the concept of obtaining information has been interpreted very broadly and has been given an expansive definition within the relevant case law. Thus, the term obtaining information "includes merely viewing information without downloading or copying a file" (ibid., 18).

Prosecuting Under US Law

Clearly, given the nature of the Night Dragon attacks and those activities alleged in the indictment, the individual perpetrator or perpetrators will have

5 See, for example, *United States v. Drew*, 259 F.R.D. 449, 457 (C.D. Cal. 2009) ("Initially, it is noted that the latter two elements of the section 1030(a)(2)(C) crime will always be met when an individual using a computer contacts or communicates with an Internet website"); *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) ("No additional interstate nexus is required when instrumentalities or channels of interstate commerce are regulated […] With a connection to the Internet, the [victim] computers were part of 'a system that is inexorably intertwined with interstate commerce' and thus properly within the realm of Congress's Commerce Clause power."); *Paradigm Alliance, Inc. v. Celeritas Technologies, LLC*, 248 F.R.D. 598, 602 (D. Kan. 2008) ("As a practical matter, a computer providing a 'web-based' application accessible through the internet would satisfy the 'interstate communication' requirement."); and *Continental Group, Inc. v. KW Property Management, LLC*, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009) ("There is a split of authority on this issue, but the greater weight of authority favors Plaintiff on this issue. A connection to the internet is 'affecting interstate commerce or communication.'").

6 18 USC § 1030(a)(2).

7 Ibid.

contravened the relevant portions of the Computer Fraud and Abuse Act, if the facts set out were proven to be true. Given the fact that the target computers were connected to the Internet, they would fall within the statutory definition of a protected computer. Moreover, there is really no debate that the Chinese attackers did not have authorization, especially given the way that they accessed the systems in question. As a consequence, it is a safe legal conclusion that these exploits were prohibited under US domestic criminal law. The relevant question then becomes, what can the United States do about it? Securing a criminal conviction is no easy feat — witnesses need to be found, evidence needs to be secured and a case needs to be marshalled.

Any successful prosecution is built on a solid evidentiary foundation and the prosecution of cybercriminals is no different. Building a successful case against any cybercriminal will require marshalling evidence, which will likely include digital evidence retrieved through forensic cyber investigation, and this forensically relevant digital information can be located in one of several countries. A rudimentary analysis would likely find relevant information on the targeted computers, systems and networks located in the United States and on the attackers' machines in China. There is certainly a possibility that relevant information could be located elsewhere, but only the foregoing will be considered for the sake of brevity and clarity of legal analysis.[8]

In a typical cyber investigation, law enforcement can employ investigative tools that fall within one of two categories — either coercive or covert techniques (Walden 2007, 203). Covert techniques, including wiretaps and clandestine surveillance, are typically employed at the early stages of an investigation and, certainly, while a crime is either ongoing or the suspects are liable to provide additional evidence. However, given that the acts found in the indictment and those committed during the Night Dragon attacks have already transpired, the use of coercive investigative tools would be the predominant mechanism employed in an attempt to bring the perpetrators to justice.

With respect to the investigation, there are at least two different jurisdictions involved and, therefore, at least two different instigative regimes will apply. With respect to the data and other forensically relevant information available on the systems that were targeted and fell victim to infiltration, one of two scenarios will be present. Either the victim corporation will cooperate with the investigation and provide system access to investigators, or they will not, requiring investigators to apply for a warrant.[9] Even if the victim company is willing to cooperate fully with investigators and this portion of the investigation yields useful evidence, that evidence may be insufficient for the purposes of a criminal prosecution.

In the case of the Night Dragon infiltration, the circumstantial evidence suggests that the attacks were not the work of one individual, but rather that it was a concerted effort of many actors working together. Notwithstanding the fact that this attack was a group effort, McAfee was able to identify one individual who provided the foundational command and control server infrastructure that facilitated the attack. According to McAfee, this individual is based in Heze City, Shandong Province, China (McAfee 2011, 18). The McAfee report went on to conclude that:

8 Communications also can be routed through a third country.

9 Some companies fail to report cyber breaches or do not cooperate with authorities because they do not want it known that they were vulnerable to cyber attack.

> Although we don't believe this individual is the mastermind behind these attacks, it is likely this person is aware or has information that can help identify at least some of the individuals, groups, or organizations responsible for these intrusions.
>
> The individual runs a company that, according to the company's advertisements, provides "Hosted Servers in the U.S. with no records kept" for as little as 68 RMB (US$10) per year for 100 MB of space. The company's U.S.-based leased servers have been used to host the zwShell C&C application that controlled machines across the victim companies.

Based on the foregoing, US authorities could form the belief that useful electronic evidence will be located on the central servers of the subject company located in Heze City, China. The same could easily be true in relation to forensic evidence in support of the indictment against the five Chinese officials. These actions, if proven, would constitute a contravention of US law. However, this exposes the difference between "prescriptive" jurisdiction and "enforcement" jurisdiction under international law, both of which will be considered in the next sections.

Extraterritorial Application of Domestic US Criminal Law

The generally applicable rule is that US law does *not* apply extraterritorially.[10] Put another way, typically the reach of US law will stop at the border. Thus, there is a legal presumption that domestic law does *not* have extraterritorial application. This presumption will only be overcome upon showing evidence of a contrary legislative intent to allow the law to apply outside of US territory.[11] Therefore, in the context of a cybercrime prosecution, the government will need to displace this legal presumption by demonstrating "clear evidence of congressional intent to apply a statute beyond our borders."[12]

In this respect, any real debate regarding the extraterritorial application of the prohibitions in section 1030 was resolved in 2001 with the passage of the USA PATRIOT Act. Under the auspices of this act, Congress revised section 1030, providing for explicit extraterritorial application of the section. To that end, the USA PATRIOT Act amended definition of a protected computer in section 1030(e)(2)(B) to specifically include a computer that "is used in interstate or foreign commerce, including a computer located outside the United States that is used in a manner that affects interstate or foreign

---

10 See Brenner and Koops (2004).

11 See *United States v. Cotten*, 471 F.2d 744, 750 (9th Cir. 1973) ("Absent evidence of a contrary intent, the presumption against extraterritorial application must stand").

12 *Equal Employment Opportunity Comm. v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991) (internal citations omitted) ("Both parties concede, as they must, that Congress has the authority to enforce its laws beyond the territorial boundaries of the United States. Whether Congress has in fact exercised that authority in these cases is a matter of statutory construction."); See also *United States v. Gatlin*, 216 F.3d 207, 211 (2d Cir. 2000).

commerce or communication of the United States."[13] Even before the passage of the USA PATRIOT Act in 2001, the United States District Court, District of Connecticut, held in *United States v. Ivanov* that "Congress has the power to apply its statutes extraterritorially, and in the case of 18 USC. § 1030, it has clearly manifested its intention to do so."[14]

As a consequence, given the plain meaning of the statute as amended by the USA PATRIOT Act and previous on-point court decisions, it seems clear that this portion of US law has international effect.[15] Thus, US law enforcement is clearly in a position where the prescriptive reach of American law prohibits these types of attacks. This fact, however, does not mean that the United States may enforce that law within the territory of another state.

Enforcement Jurisdiction

Clearly, US law permits the prescriptive extraterritorial application of section 1030. This does not, however, allow the extraterritorial enforcement of this provision.[16] In attempting to prosecute the case under indictment or the Night Dragon offences, US authorities would be required to seek assistance from the relevant Chinese authorities in order to enforce US law against those perpetrators located in China. Thus, "in general, law enforcement officers exercise their functions in the territory of another country only with the consent of that country" (DoJ, n.d., "Searching and Seizing Computers").

Therefore, according to the manual, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," published by the Computer Crime and Intellectual Property section of the DoJ, law enforcement should only contact an Internet service provider located in a foreign jurisdiction in one of three circumstances: they have obtained the prior permission of the foreign government; they have obtained the approval of the DoJ's Office of International Affairs (OIA), which will be familiar with the accepted practices regarding the subject state; or there are other "clear indicia" that this type of investigative practice would not be "objectionable" within the subject state (ibid., 57).

According to the DoJ, the current view of the United States is that law enforcement will not be required to obtain the prior consent of the subject state,

13 18 USC § 1030(e)(2)(B).

14 *See United States v. Ivanov*, 175 F. Supp. 2d 367, 375 (D. Conn. 2001).

15 The United States may also extend extraterritorial jurisdiction based on detrimental effects that take place within the United States. See *United States v. Muench*, 694 F.2d 28, 33 (2d Cir. 1982) ("The intent to cause effects within the United States also makes it reasonable to apply to persons outside United States territory a statute which is not extraterritorial in scope."); *United States v. Steinberg*, 62 F.2d 77, 78 (2d Cir. 1932) ("It has long been a commonplace of criminal liability that a person may be charged in the place where the evil results, though he is beyond the jurisdiction when he starts the train of events of which that evil is the fruit.").

16 See Randall (1988, 785-86). ("The term 'jurisdiction' refers to the legitimate assertion of authority to affect legal interests. Jurisdiction may describe the authority to make law applicable to certain persons, territories, or situations (prescriptive jurisdiction); the authority to subject certain persons, territories, or situations to judicial processes (adjudicatory jurisdiction); or the authority to compel compliance and to redress noncompliance (enforcement jurisdiction). There are five bases of jurisdiction recognized under international law: territorial (based on the location of the acts or effects), nationality (based on the citizenship of the accused), passive personality (based on the citizenship of the victim), protective (based on essential security interests), and universal"). See also Scharf (2012, 357, 365).

provided the investigation is limited to publicly available materials (i.e., a website, Twitter feed or blog) or the investigating authorities have obtained the voluntary consent of a person who has lawful authority to disclose the subject materials (ibid.). In the event that neither of these circumstances exists, US authorities will be required to cooperate either informally with foreign authorities or they will have to pursue mutual legal assistance through formalized channels.

In the event that the activity taking place contravenes the law in both the United States and in a foreign state, enforcement authorities may be able to share evidence "informally" with US investigators; this sharing is obviously subject to evidentiary concerns related to the chain of custody and the need to have a witness who can testify in open court as to where the information came from. However, finding the appropriate official with "which to explore such cooperation is an inexact science, at best" (ibid.). In addition, there is deep suspicion on the part of both the United States and China in the realm of cyber relations.[17] Thus, the more likely scenario is that US law enforcement would be required to pursue cooperation through formal channels. In this respect, when trying to secure evidence related to these cyber attacks, US authorities would have to rely on the mutual legal assistance treaty that is in force between the two states, which will be considered in greater detail below.[18]

Chinese Cyber Law and Strategic Interests

If the United States has a well-developed, robust and sophisticated legal regime prohibiting a range of injurious cyber conduct, then China has its mirror opposite. The entire portion of the criminal law dedicated to prohibiting unwanted cyber conduct is encapsulated in three brief legislative articles. Given the brevity of these prohibitions, they will be set out in their entity and then analyzed below. The relevant portions of the Criminal Law of the People's Republic of China (1997) provide:

> Article 285
>
> Whoever, in violation of state's stipulations, invades a computer information system involving the fields of state affairs, national defence construction or most advanced science and technology shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention.
>
> Article 286
>
> Whoever, in violation of state's stipulations, deletes, amends, adds or disturbs functions of a computer information system and causes the computer information system's inability to work normally shall, if serious consequences exist, be sentenced to fixed-term imprisonment of not more than

17 See Institute of Global Conflict and Cooperation (2012, 1). "In recent years the security of global information systems has become a contentious issue in U.S.–China relations. U.S. government sources allege that Chinese intrusions targeting proprietary economic data and sensitive national security information are on the rise. At the same time, a large proportion of malicious activity globally originates from computer hosts located in the United States. Both the U.S. Department of Defense and the Chinese People's Liberation Army (PLA) view cyberspace as a new domain of conflict, and they eye each other warily."

18 Agreement Between the Government of the People's Republic of China and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, US-PRC, June 19, 2000.

> five years or criminal detention. If especially serious consequences exist, the offender shall be sentenced to fixed-term imprisonment of not less than five years.
>
> Whoever, in violation of state's stipulations, conducts operations of deletion, amendment or addition towards data or application programmes which are stored, disposed of or transmitted in a computer information system shall, if serious consequences exist, be punished according to the provisions of the preceding paragraph.
>
> Whoever intentionally makes or disseminates computer virus or other destructive programmes and affects the normal operation of a computer information system shall, if serious consequences exist, be punished according to the provisions of the first paragraph.
>
> Article 287
>
> Whoever uses a computer to practise a financial fraud, theft, embezzlement, misappropriation of public money, to steal state secrets or to commit other crimes shall be decided a crime and punished according to the relevant provisions of this Law.

These jail sentences are exceedingly light for a country that routinely hands out double-digit jail terms for journalists, artists and academics who are critical of the ruling party. Moreover, it is not clear from the wording of the above provisions if these prohibitions apply only within Chinese territory or if they would capture the conduct of a person in China attacking a system located on foreign soil. As a consequence, this appears to be an exceedingly weak legal framework. This has been attributed to the notion that China is in the early stages of legislative development. In this regard:

> Cybercrime legislation in China is still in the very early stages of development. Substantive criminal law, supplemented by commercial and intellectual property protection law, may prohibit a range of misconduct directed towards or involving computers. However, gaps and inadequacies in traditional offence provisions necessitate the consideration of more specific laws targeting cybercrimes. (Qi, Wang and Xu 2009, 219)

However, there is a less innocent — and probably more accurate — explanation for the lack of an effective legal structure within China: it is not in the short-run interests of the Chinese state to pursue a robust legal regime that combats international cybercrime. According to a recent report from the US Office of the National Counterintelligence Executive, the Chinese have a strategic interest in economic exploitation. In this respect, Chinese leaders consider the first two decades of the twenty-first century to be a "window of strategic opportunity" (Office of the National Counterintelligence Executive 2011, 15).

The Chinese government and Chinese companies have a significant incentive to engage in economic espionage. Additionally, given the technical difficulties related to attribution, they can engage in wholesale electronic espionage with little serious risk of reprisal. This threat from Chinese cyber attack is not unique to the United States. Given the nature of China's strategic interests, other Western states have been identified as targets as well. In the

United Kingdom, a document from MI5 called "The Threat from Chinese Espionage" said that "'any UK company might be at risk if it holds information which would benefit the Chinese.' Furthermore, the report describes how China's cyber warfare campaign had targeted British defense, energy, communications and manufacturing companies, as well as public relations and international law firms, some of them being a vital part of the British critical infrastructure" (Hjortdal 2011, 7).

These cyber attacks are a major expression of Chinese strategic policy. In another forum, James A. Lewis, from the Center for Strategic and International Studies, made several comments that are particularly apt: "This is a big espionage program aimed at getting high-tech information and politically sensitive information — the high-tech information to jump-start China's economy and the political information to ensure the survival of the regime…This is what China's leadership is after. This reflects China's national priorities" (quoted in Cha and Nakashima 2010, A1). Given the strategic interest in engaging in electronic espionage, informal cooperation with US authorities would be unlikely; therefore, US authorities would have to seek recourse to the formalized mechanisms of international law.

International Law

Significant international efforts have been made to combat crimes committed via the Internet. These efforts have culminated in the Council of Europe's Convention on Cyber Crime, which has a broad subject matter, dealing with infringements of copyright, computer-related fraud, child pornography and violations of network security.[19] It also contains a series of powers and procedures, such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, in particular by adopting appropriate legislation and fostering international cooperation. While the United States is a state party to the convention, China is not. As a consequence, the provisions of the convention have no bearing on the domestic prosecution of, or international cooperation related to, the activities alleged in the indictment or the Night Dragon attacks. That is not to say, however, that international law is irrelevant in this context.

As noted, there is a mutual legal assistance treaty between the United States and China, which is considered to be a legally binding international agreement. The provisions of the treaty are quite wide-ranging, covering, for example: making persons available to give evidence or assist in investigations; locating or identifying persons; executing requests for inquiry, searches, freezing and seizures of evidence; assisting in forfeiture proceedings; and transferring persons in custody for giving evidence or assisting in investigations.[20]

In order to initiate the process for trying to secure forensically relevant digital evidence, a formal request would be made by the OIA to the designated "central authority" of China, who is named in the mutual assistance treaty as the Ministry of Justice. Therefore, according to the DoJ manual, when US law enforcement has reason to believe that electronic evidence exists on a computer or computer network located in a foreign jurisdiction, a request to foreign law enforcement for preservation of the evidence should be made as soon as possible; such a request "will have varying degrees of success based on

19 The convention is available on the website of the Council of Europe at http://conventions.coe.int/Treaty/en/Treaties/ Html/185.htm.

20 Agreement between the Government of the People's Republic of China and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, US-PRC, June 19, 2000.

several factors" including whether the country in question has "a data preservation law and whether the U.S. has sufficient law enforcement contacts… to ensure prompt execution of the request" (DoJ, n.d., "Searching and Seizing Computers," 58). There is also a wide set of exemptions under the mutual assistance treaty that will allow either the United States or China to greatly limit the assistance that it is obliged to render pursuant to the treaty. In this regard, a party may deny assistance if the request relates to conduct that would not constitute an offence under the laws in the territory of the "requested party" or the execution of the request "would prejudice the sovereignty, security, public order (ordre publique), important public policy or other essential interests of the Requested Party."[21]

In this way, any assistance that China would be obligated to provide is limited in two important respects. First, there is a dual criminality provision, meaning that the impugned conduct must be illegal in both states. Given the lacklustre status of Chinese domestic criminal law related to cyber offences, it is not entirely clear if the existing laws govern conduct that has extraterritorial effect, or if the law simply regulates acts aimed at domestic Chinese computer systems and equipment. Second, a state is not obliged to render legal assistance if rendering that assistance would prejudice its sovereignty or security. There is little doubt that if a request for legal assistance was put forward by the United States, it would be rebuffed on these grounds.

CONCLUSION

This paper has attempted to highlight the need for enhanced international cooperation in order to effectively combat the global menace of cybercrime. This area of Internet governance, like others, is in need of enhanced international and transnational legal cooperation. In fact, this enhanced cooperation is a necessary condition for the effective prosecution of cybercriminals on any meaningful level. However, there are a number of political and geostrategic reasons why this enhanced cooperation is unlikely to be forthcoming among a number of the major state players in this area. The examples of the recent indictment of five Chinese officials by the DoJ and the Night Dragon computer attacks highlighted some of these challenges.

There is a broader set of interests at play as well. The fact that a number of governments routinely engage in economic cyber espionage and cybercrime erodes digital trust within the larger stakeholder community. The Internet is the greatest communication, wealth generation and social networking tool ever created. However, much of this success is based on the relative stability and security of the platform, and the activities of various governments have a tendency to erode those values.

The view of certain governments that economic espionage and crime are in their strategic interest is short sighted. The unearthing of these activities will provoke a negative response by the victim state and has the potential to destabilize and erode relations between governments. Such activities require companies to take additional, often costly steps, to secure their networks and data. They undermine consumer confidence and infiltrations can affect both stock prices and the profitability of companies. A safe, secure and responsibly governed Internet is, therefore, in the long-term strategic interest of most, if not all, states. The game that a number of states are playing in this area is reckless and foolhardy.

It is reckless because employing a policy of economic cyber espionage and cybercrime as a mechanism for advancing narrow national economic interests holds the potential to undermine trust in the system. This is a major problem because the Internet has been

21 Ibid.

such a force for economic growth precisely because everyone from individuals to enterprise trusts the security of online transactions. The degradation of that trust could have long-term financial drawbacks. In addition, cybercrime places a burden on the global economy by redirecting lawful earnings into the criminal underworld. Recent estimates place the annual cost from cybercrime to the global economy at over US$400 billion (Center for Strategic and International Studies 2014). As the Internet becomes even more ubiquitous and society moves to the "Internet of everything," where cars, refrigerators, homes and so on are connected, the points of vulnerability increase, as well as the potential economic impact.

It is foolhardy because by fostering these types of policies, governments may be undermining their long-term economic interests in favour of short-term gain. If security vulnerabilities continue to be exploited and economic exposure becomes more problematic, it will create barriers to electronic commerce. This will, at a minimum, create an unwanted economic drag. However, if, as some have suggested, there was ever a massive surprise digital attack against critical infrastructure similar to the Japanese attack on Pearl Harbor in 1941, colloquially called a "digital Pearl Harbor," it could destabilize the global economy. The implications of this would be profound. As major governments foment policies of digital snooping to gain competitive economic advantage, the risk of destabilizing events continues to increase.

This paper began by highlighting the need for increased cooperation among governments in order to combat the global menace of cybercrime; however, this cooperation is unlikely to occur as long as the discourse surrounding cybercrime remains so heavily politicized and securitized. Governments are not likely to come together if they view others as their adversaries and as a security threat. A conceptual reorientation that articulates a view of cybercrime as a threat to the global economy, not to individual states, and as an economic, not a security, issue is needed. If governments coalesced around the notion of trying to prevent the long-term degradation of trust in the online economy, they may profitably advance the dialogue away from mutual suspicion and toward mutual cooperation.

WORKS CITED

Associated Press. 2014. "China Demands Halt to 'Unscrupulous' US Cyber-spying." *The Guardian*, May 27. www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying.

BBC News. 2013. "US-China Cyber Security Working Group Meets." BBC News. July 8. www.bbc.com/news/world-asia-china-23177538.

Brenner, Susan and Bert-Jaap Koops. 2004. "Approaches to Cybercrime Jurisdiction." *Journal of High Technology Law* 4 (1).

Center for Strategic and International Studies. 2014. "Net Losses: Estimating the Global Cost of Cybercrime." June. http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

Cha, Ariana Eunjung and Ellen Nakashima. 2010. "Google Attack Part of Vast Campaign; Targets Are of Strategic Importance to China, where Scheme Is Thought to Originate." *The Washington Post*, January 14.

Deibert, Ronald J. 2013. *Bounding Cyber Power: Escalation and Restraint in Global Cyberspace*. Internet Governance Paper Series No. 6.

DoJ. 2014. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." May 19. www.justice.gov/opa/pr/2014/May/14-ag-528. html.

———. n.d. "Prosecuting Cyber Crimes." Computer Crime and Intellectual Property Section Criminal Division, Office of Legal Education Executive Office for United States Attorneys.

———. n.d. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." Computer Crime and Intellectual Property Section Criminal Division, Office of Legal Education Executive Office for United States Attorneys.

Hathaway, Oona A. 2012. "The Law of Cyber-Attack." *California Law Review* 100.

Hjortdal, Magnus. 2011. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4 (2): 1–24.

Institute of Global Conflict and Cooperation. 2012. "China and Cybersecurity: Political, Economic, and Strategic Dimensions." Report from Workshops held at the University of California, San Diego. April.

Jones, Terril Y. 2013. "U.S., China Agree to Work Together on Cyber Security." Reuters. April 13. www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413.

Lewis, James A. *Internet Governance: Inevitable Transitions*. Internet Governance Paper Series No. 4.

Marion, Nancy E. 2010. "The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation." *International Journal of Cyber Criminology* 4 (1 and 2): 699–712.

McAfee Foundstone Professional Services and McAfee Labs. 2011. "Global Energy Cyberattacks: 'Night Dragon,'" February 10.

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.

Office of the Secretary of Defense. 2013. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013." US Department of Defense. www.defense.gov/pubs/2013_china_report_final.pdf.

Qi, Man, Yongquan Wang and Rongsheng Xu. 2009. *Fighting Cybercrime: Legislation in China. International Journal Electronic Security and Digital Forensics* 2 (2): 219–227.

People's Republic of China. 1997. "Criminal Law of the People's Republic of China." The National People's Congress. Order of the President of the People's Republic of China. No. 83. www.asianlii.org/cn/legis/cen/laws/clotproc361/.

Randall, Kenneth C. 1988. "Universal Jurisdiction under International Law." *Texas Law Review* 66.

Scharf, Michael P. 2012. "Universal Jurisdiction and the Crime of Aggression." *Harvard International Law Journal* 53: 357–389.

Schmidt, Michael S. and David E. Sanger. 2014. "5 in China Army Face U.S. Charges of Cyberattacks." *The New York Times*, May 19. www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?module=Search&mabReward=relbias%3As.

Sinrod, Eric J. and William P. Reilly. 2000. "Cyber-crimes: A Practical Approach to the Application of Federal Computer Crime Laws." *Santa Clara Computer & High Tech Law Journal* 16: 177–232.

Sofaer, Abraham D. and Seymour E. Goodman. 2011. "Cyber-Crime and Security: The Transnational Dimension." In *The Transnational Dimension of Cyber Crime and Terrorism*, edited by Abraham D. Sofaer and Seymour E. Goodman, 1–34. Stanford: Hoover Institution Press.

Walden, Ian. 2007. *Computer Crimes and Digital Investigations*. Oxford: Oxford University Press.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on four themes: the global economy; global security; the environment and energy; and global development.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

CIGI MASTHEAD

Managing Editor, Publications
Carol Bonnett

Publications Editor
Jennifer Goyder

Publications Editor
Vivian Moser

Publications Editor
Patricia Holmes

Media Designer
Steve Cross

EXECUTIVE

President
Rohinton Medhora

Vice President of Programs
David Dewitt

Vice President of Public Affairs
Fred Kuntz

Vice President of Finance
Mark Menard

COMMUNICATIONS

Communications Specialist
Kevin Dias
kdias@cigionline.org
1 519 885 2444 x 7238

Public Affairs Coordinator
Erin Baxter
ebaxter@cigionline.org
1 519 885 2444 x 7265

57 Erb Street West
Waterloo, Ontario N2L 6C2, Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org