Pattern of global cyber war and crime: A conceptual framework

Article *in* Journal of International Management · December 2005

DOI: 10.1016/j.intman.2005.09.009

1 author:

Nir Kshetri
University of North Carolina at …

174 PUBLICATIONS **1,335** CITATIONS

ELSEVIER

Journal of International Management
11 (2005) 541–562

THE FOX SCHOOL of Business and Management
TEMPLE UNIVERSITY

Pattern of global cyber war and crime: A conceptual framework

Nir Kshetri *

Bryan School of Business and Economics, The University of North Carolina at Greensboro, Bryan Building, Room: 368, P.O. Box 26165, Greensboro, NC 27402-6165, USA

Received 14 December 2004; accepted 14 September 2005

Abstract

The flourishing synergy arising between organized crimes and the Internet has increased the insecurity of the digital world. How hackers frame their actions? What factors encourage and energize their behavior? These are very important but highly underresearched questions. We draw upon literatures on psychology, economics, international relation and warfare to propose a framework that addresses these questions. We found that countries across the world differ in terms of regulative, normative and cognitive legitimacy to different types of web attacks. Cyber wars and crimes are also functions of the stocks of hacking skills relative to the availability of economic opportunities. An attacking unit's selection criteria for the target network include symbolic significance and criticalness, degree of digitization of values and weakness in defense mechanisms. Managerial and policy implications are discussed and directions for future research are suggested.

Keywords: Information and communications technologies; Cyber war; Hacking; Mafia; Nationalism

1. Introduction

Information and communications technologies (ICTs) have drastically increased the porosity between national borders (Rosenau, 1995). The increased porosity and anonymity[1] of the Internet

* Tel.: +1 336 334 4530; fax: +1 336 334 4141.
E-mail address: nbkshetr@uncg.edu.

[1] Unlike in the traditional warfare, it is almost impossible to identify the attacker in the IT warfare. Victims may not know whether an attacker is a teenager or terrorist, a rival company or a foreign government. In the famous Storm Cloud case, for instance, U.S. officials were not able to determine whether a foreign government or maverick hackers were involved (Bridis, 2001).

1075-4253/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.intman.2005.09.009

superimpose in a complex interaction that enables criminal and violent groups, transnational terrorist organizations, and companies engaged in espionage to expand their operations globally. Government backed cyber-terrorism in some countries (Comité Européen Des Assurances, 2004) and maverick hackers testing their skills have further threatened the digital world.

The flourishing synergy between organized crimes and the Internet (Williams, 2001) has thus increased the insecurity of the digital world. The U.S. Federal Bureau of Investigation (FBI) reports that cyber criminals have attacked almost all of the Fortune 500 companies.[2] According to the market research firm, International Data Corporation (IDC), 39% of Fortune 500 companies suffered a security breach in 2003 and 40% of global IT managers have rated security as their number one priority. Hackers have attacked computer networks of the Pentagon and the White House, NATO's military websites and have stolen secret source codes of Microsoft and credit card numbers from a number of U.S. banks (Lunev, 2001; Walker, 2004). Cybercrime and cyber-terrorism are currently the FBI's No. 3 priority-behind counterterrorism and counterintelligence (Verton, 2002).

With rapid digitization of businesses and increasing web attacks (Carblanc and Moers, 2003), organizations rightfully worry about the security of their networks. A deeper and richer understanding of the principles and purposes; necessary and sufficient conditions for web attacks (Coates, 2002); and the patterns of origin and targets would help managers as well as national and international policy makers devise strategies to combat such crimes. Nonetheless, no published study has addressed such an important issue. To fill the research gap and to initiate further academic discussion on this topic, we integrate streams of literatures from psychology, economics, warfare and international affairs to develop a model on the pattern of global cybercrimes.

We define a cybercrime (or a cyber attack) broadly as any crime that employs a computer network in any phase of the crime. Examples of cybercrimes include critical infrastructure attack, fraud, online money laundering, criminal uses of Internet communications, ID fraud, use of computers to further traditional crimes and cyber extortions. The remainder of the paper is structured as follows: The next section provides a brief survey of digital security threat. Then, we propose a model that explains sources, targets, motivations and types of web attacks. Finally, we provide discussions and implications.

2. Digital security threat: a brief survey

Estimating economic impacts of web attacks to a reasonable level of accuracy at the global level has been a challenge. Since many web attacks go unreported, such impacts tend to be underestimated. Triangulation of data from different sources indicates substantial economic losses of the global cyber attacks. The Council of Europe estimated the annual cost of repairing damages caused by computer viruses at $12 billion[3]. In 2003, U.S. consumers and businesses lost over $14 billion in three categories of digital crimes (spam: $10 billion; cost of fraud to online merchants: $2 billion; fraudulent e-mails and websites designed to trick consumers to reveal personal information or phishing: $2 billion) (Swartz, 2004). More alarming perhaps is online credit card fraud. According to the FBI, 30 million credit card numbers were stolen

[2] See "Reducing On-line Credit Card Fraud," *Web Developers Journal*, http://www.webdevelopersjournal.com/articles/card_fraud.html, http://www.fbi.gov/publications/leb/2002/june2002/june02leb.htm (accessed February 27, 2005).

[3] See Cyber Terrorism: The Growing Threat, http://www.ecssr.ac.ae/CDA/en/FeaturedTopics/DisplayTopic/0,1670,296,00.html.

Table 1
Top sources of cybercrimes

Countries from which most online fraud originates[a]	Rank of countries according to % of orders that U.S. sites declared as fraudulent[b]	Rate of attacks per 10,000 Internet users (First half 2004)[c]	Number of attacks per 10,000 Internet users (First half 2002)[d]	Percent of total attacks (First half 2002)[d]
Ukraine	Yugoslavia	Latvia	Kuwait (50.8)	USA (40)
Indonesia	Nigeria	Macau	Israel (33.1)	Germany (7.6)
Yugoslavia	Romania	Israel	Iran (30.8)	South Korea (7.4)
Lithuania	Pakistan	Australia	Peru (24.5)	China (6.9)
Egypt	Indonesia	Finland	Chile (24.4)	France (5.2)
Romania	Macedonia	Egypt	Nigeria (23.4)	Canada (3.0)
Bulgaria	Bulgaria	Turkey	Morocco (22.3)	Italy (2.7)
Turkey	Ukraine	Spain	Hong Kong (22.1)	Taiwan (2.4)
Russia	Lebanon	Canada	Puerto Rico (20.8)	UK (2.1)
Pakistan	Lithuania	Nigeria	France (19.9)	Japan (2.1)
Malaysia			Argentina (19.3)	
Israel			Belgium (17.6)	
			Romania (16.5)	

[a] International Fraud Watch (Online Fraud Stats http://www.ocalasmostwanted.com/online_fraud_stats.htm).
[b] Merchant Risk Council: Sullivan (2004).
[c] Symantec (2004, p. 17).
[d] Riptech (2002).

through computer-security breaches during 1999–2003, resulting in $15 billion in losses (also see Box 2). The U.S. Secret Service calls credit card fraud "the bank robbery of the future".[4] What is more, a number of purely symbolic cyber attacks (e.g., those directed towards challenging some forms of ideologies) also entail significant economic losses.[5]

Who are the cyber attackers? A survey conducted among the members of the Confederation of British Industry indicated that the attackers in the most serious cybercrimes in 2000 were hackers (44.8%), former employees (13.4%), organized criminal groups (12.8%), current employees (11.5%), customers (7.9%), competitors (5.8%), political and protest groups (2.6%) and terrorists (1.4%) (BBC News 2001). A large proportion of such attacks are international in scope (Table 1). A 2002 survey of Australian firms indicated that foreign governments were perceived sources of attacks for 24% respondents and foreign corporate for 30% (Deloitte Touche Tohmatsu, 2002).

Although the US is the No. 1 source country for web attacks, its share in the global cybercrime industry is decreasing rapidly. The proportion of attacks originated from the US dropped from 58% in the second half of 2003 to 37% in the first half of 2004 (Symantec, 2004). It should, however, be noted that the country of origination of a cyber attack is extremely fuzzy. Many cybercrimes originate in one country but are initiated by attacking units in different territories. For instance, in 1999, two members of a US-based "Phonemasters" were convicted for attacking the networks of U.S. telecomm companies. One of them downloaded thousands of Sprint calling card numbers that were sold to intermediaries in Canada and Switzerland and finally ended up with an organized group in Italy (Williams, 2001). Similarly, a hacker accused of pirating DirecTV and EchoStar signals in Florida told law enforcement authorities that he had

[4] Fraud prevention for the online enterprise, http://www.quova.com/solutions/internet-fraud-detection.shtml.
[5] For instance, hackers that attacked India's Bhabha Atomic Research Center (BARC) network in 1998 also downloaded thousands of pages of e-mail and research documents and erased huge amount of data (Denning, 2000).

received request from Afghanistan to provide hacking services (Lieberman, 2003). In the same vein, ShadowCrew, the international clearinghouse for stolen credit cards and identity documents, whose masterminds were arrested in the US in the mid-2005, had 4000 members in a number of countries including Bulgaria, Canada, Poland, Sweden and the US (Grow and Bush, 2005). Likewise, Australian scammers have established links with Russian and Malaysian organized crime networks to transfer stolen money from overseas banks they have cracked into (Foreign Policy, 2005).

Targeted web attacks are not limited to networks of large organizations. Such attacks accounted for 10% of total attacks in small businesses in the first half of 2004 compared to 3% in the second half of 2003 (Symantec, 2004, p. 17).

Table 1 ranks the world's top nations in terms of cyber attacks and frauds on the Internet. One estimate suggests that less than 1% of computer attacks originate in countries that the US considers breeding grounds for terrorists and hackers (The Economist, 2003). Another estimate suggests that 60% of fraudulent transactions originate from just 15 nations.[6]

3. Pattern of the global cyber war and crime: a proposed model

Our proposed model on the pattern of global cyber attacks is presented in Fig. 1. Although the model entails different levels of analysis, it helps us understand the mechanisms connecting sources and targets. In this section, we briefly discuss building blocks of the model.

4. Characteristics of the source nation

4.1. Institutions

An examination of institutions in which a hacking unit is embedded helps us to understand the sources of regulative, normative and cognitive legitimacy of hackers' actions. Viewing from a rational perspective, institutions are mechanisms that provide efficient solutions to predefined problems (e.g., decision regarding involvement in hacking activities and choice of a website to attack) (Olson, 1965; Williamson, 1975). Institutions do so by helping align individual and collective interests. North (1990) defines institutions as macro-level rules of the game and thus distinguishes the players (organizations) from the rules (institutions) (p. 27). The rules can be formal as well as informal. Scott (1995) has viewed institutions as composed of three broad categories: regulative, cognitive, and normative. Each set can be mapped with corresponding legitimacy concerns.

4.2. Regulative institutions

Regulative institutions consist of "explicit regulative processes: rule setting, monitoring, and sanctioning activities" (Scott, 1995, 35). In the context of this paper, regulative institutions consist of regulatory bodies (such as the U.S. Department of Justice) and existing laws and rules that influence computer hackers to behave in certain ways (Scott, 1995). In this section, we discuss the influence of regulative institutions in terms of *rules* and *rule-making bodies*.

[6] Fraud prevention for the online enterprise, http://www.quova.com/solutions/internet-fraud-detection.shtml.

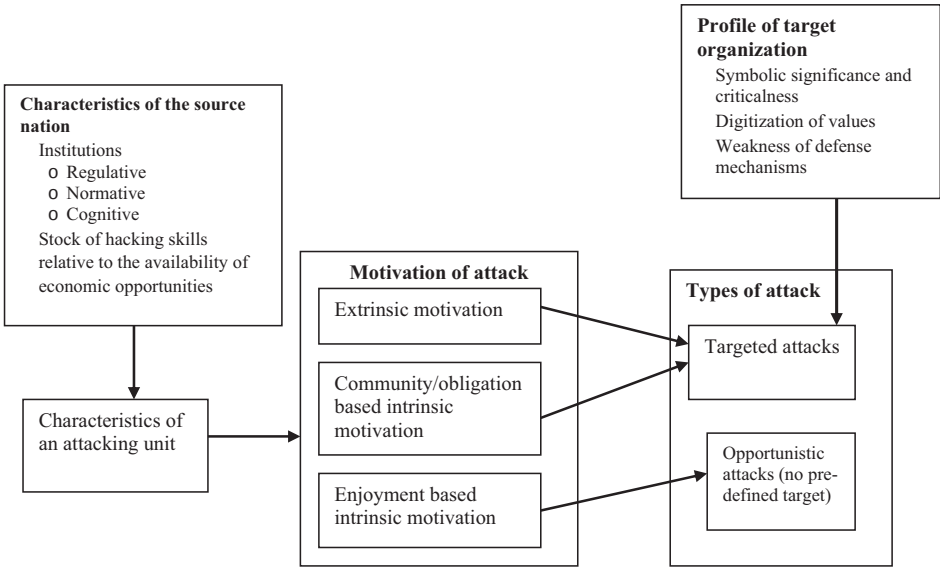

Fig. 1. Understanding the pattern of the global cyberattacks: a proposed framework.

4.3. Rules (strength of rule of law)

Cyber attacks have benefited from jurisdictional arbitrage. Ceteris paribus, the lack of a strong rule of law is associated with origination of more cyber attacks (see Boxes 1 and 2). Put differently, organized cybercrimes are initiated from countries that have few or no laws directed against cybercrimes and little capacity to enforce existing laws (Williams, 2001, also see Table 1). For instance, when a Filipino hacker launched the "Love Letter" virus in 2000, estimated loss of damage in the US was in the range of $4–15 billion. But the U.S. government could not do anything to prosecute the hacker or to recover the damages because at that time the Philippines had no laws prohibiting such crimes (Adams, 2001).

Box 1
Internet-led internationalization of Russian Mafia

The Internet can play a critical role in enhancing an organization's market reach and operational efficiency (Porter, 2001). Some organizations are more compatible (Rogers, 1983) with the Internet and hence are more likely to benefit from the increased reach and efficiency created by the digital technology. In particular, Mafia's work style and prior work experience seem to be compatible with the Internet.

According to Diego Oambetta, the Mafia is a profit-focused firm selling private protection (1988, 130). Legal as well as illegal businesses in Russia were required to buy the dispute-resolution and contract-enforcement "services" of the Mafia and to pay fees to protect their business and even to remain alive (Handelman, 1999; Varese, 2002). With rapid digitization of values and organizations' increased dependence on digital technology worldwide, Mafia groups have realized huge financial potential of the Internet.

The fragile property rights, too weak state (Varese, 2002), inefficient police[7] and weak cybercrime laws (Onlinecasinonews.com, 2004) have provided a fertile ground for Mafia's digital world. Although it is illegal under Russian law to hack into computer systems, few cases are prosecuted (Lorek, 2001). Russian Mafia hack rings are reportedly operated by former KGB agents.[8] The police said most hackers are young and educated, work independently and do not fit police profiles of criminals.[9]

Mafia groups have now digital versions of bombings, murders, kidnappings and hijackings. They carefully plan attacks in terms of the target, the time and the amount of extortion. In most cases, they demand much less than the costs to repair a broken site (Walker, 2004). Many firms choose to comply with hackers' demand rather than taking the risk of attack and losing all customers and profits in one massive attack. The FBI found that in many cases extortions were paid off. For instance, online sports books, BETWWTS, reportedly paid Mafia extortionists thousands of dollars (Walker, 2004). Internet betting sites, financial institutions and e-commerce firms are the red hot targets.

Hackers that attacked Internet betting sites before American football's Super Bowl in January 2004 were based in Eastern Europe and Russia (Onlinecasinonews.com, 2004). Online gambling websites are targeted due to the time-specific nature of services (Walker, 2004). In the late 2003 and early 2004, the FBI and National Hi-Tech Crime units discovered that computer hackers employed by Russian Mafia launched a DOS attack[10] on Worldpay[11] System that affected thousands of online casinos. VIP Management Services website was first targeted in September 2003 and was regularly attacked since then (Walker, 2004). In January, 2004, the company received an email demanding $30,000 via Western Union or to risk an attack (Onlinecasinonews.com, 2004).

Similarly, in January 2000, an unknown Russian hacker stole 300,000 credit card numbers from CD Universe and distributed 25,000 of them on a website after the U.S. retailer refused to pay a $100,000 ransom (CNN.Com, 2000). The hacker claimed that he used some of the credit card numbers to get money. In 2001, FBI reported that 40 businesses in 20 U.S. states were hit by hacker rings working in Russia and the Ukraine, and that more than a million credit card numbers had been stolen (Gomes and Bridis, 2001). The hacker issued blackmail threats, some of which exceeded $100,000 (Forensic Accounting Review and Computer Security Digest, 2001; Kshetri, 2005). FBI officials said many more companies might have been attacked without reporting the matter to authorities.

[7] Hackers—the new breed of gangsters, August 3, 2004, http://newpaper.asia1.com.sg/top/story/0,4136,69503-1-1098892740,00.html.

[8] Also see http://members.optushome.com.au/cmrc/files/AFM/Law%20in%20the%20digi/THE_PROSECUTION_OF_COMPUTER_.rtf.

[9] Hackers—the new breed of gangsters, August 3, 2004, http://newpaper.asia1.com.sg/top/story/0,4136,69503-1-1098892740,00.html.

[10] There are two categories of DoS attacks: Operating System (OS) attacks, and Network attacks. OS attacks entail discovering holes in the security of the OS and bringing down the system. Network attacks disconnect a network from the Internet services provider (ISP). The attackers use mis-configured networks to perform such attacks (See "Help! I am being DoS'ed" at http://www.irc-junkie.org/content/a-DoS.php).

[11] Online casinos rely on Worldpay to process customer's transactions and pay off gamblers (Walker, 2004).

Russia has a highly educated workforce, programming skills and a hacking friendly environment. Unavailability of other economic opportunities has forced educated computer wizards to work in the electronic underground. A self-described hacker from Moscow confessed to reporters: "Hacking is one of the few good jobs left here" (Walker, 2004). Specialized training schools teach hacking skills. Russian hackers perform sophisticated attacks with limited computer power and inexpensive software (Walker, 2004). 82% of respondents participating in a worldwide poll conducted on a hacker-oriented website indicated that Russia had the world's best computer hackers (Walker, 2004).

Although Russia has signed an agreement to help the US in investigating some crimes and computer crimes are not among them (Lemos, 2001). In 2001, the U.S. Department of Justice requested the assistance from Russian authorities but there was no response (Lemos, 2001).

Box 2
Indonesia's electronic underground

Credit card fraud has been pervasive in Indonesia. Estimates suggest that over 20% of Internet credit card transactions in Indonesia are fraudulent (Tedjasukmana, 2002) which are valued at $6 million a year (Darmosumarto, 2003).

Users of stolen credit card information (known as carders) buy a wide range of items on the Internet from foreign countries (de Kloet, 2002). Warnets, the Indonesian version of Internet cafes, are a popular means of accessing the Internet for those who do not have home connections. In order to attract customers, many Warnets reportedly provide files with a list of credit card numbers as a special service (de Kloet, 2002). Although some frauds are detected, there are instances of success. For example, a carder ordered a Harley Davidson motorcycle on the Internet and was able to receive it. The motorcycle was delivered to the carder after he bribed government officials (de Kloet, 2002).

Many Indonesian hackers feel that cyber fraud is 'wrong' but acceptable, especially if the credit card owner is rich and not an Indonesian. A carder reportedly said: "Yes, it's wrong but it really only hurts other rich countries that were dumb enough to let us. Why should an Indonesian get arrested for damaging American business?" (Shubert, 2003). Another carder said: "I only choose those people who are truly rich. I'm not comfortable using the money of poor people. I also don't want to use credit cards belonging to Indonesians. Those are a carder's ethics" (Antariksa, 2001, p. 16).

Indonesia has been consistently rated among the top nations in terms of fraudulent activities on the Internet (Table 1). U.S. online merchants consider Indonesia as one of the high-risk countries and block all orders from the country (Richmond, 2003). Indonesia was banned for some time from e-Bay auctions after a carder manipulated sellers under a false identity and card number (Lim, 2001).

Indonesian police say they lack expertise and resources to fight against cybercrimes (Tedjasukmana, 2002). Moreover, due to a lack of cybercrime

laws, Indonesian police use a 'red book', a manual to conduct credit card investigations available since 1997, to handle Internet credit card fraud (Darmosumarto, 2003). Only 15% of reported incidents are actually investigated (Shubert, 2003).

A country with a strong rule of law, on the other hand, has "sound political institutions, a strong court system" and citizens that are "willing to accept the established institutions and to make and implement laws and adjudicate disputes" (International Country Risk Guide, 1996). Put differently, a strong rule of law is characterized by effective punishment to transgressors and sanctions against defectors and thus enhances the ability to successfully litigate fraudulent dealings on the Internet (Oxley and Yeung, 2001). A strong rule of laws thus provides negative motivations for hackers.

Eastern Europe and Russia's weak cybercrime laws have provided a fertile ground for computer crimes. Notwithstanding many Eastern Europe countries[12] enactment of cybercrime laws, they lack enforcement mechanisms (see Box 1 for Russia). The discussion in this section is summarized as:

Proposition 1. *Ceteris paribus*[13]*, the rate of origin of online attacks in an economy is negatively related to the strength of rule of laws applied to such attacks*.

4.4. Normative institutions

Normative components introduce "a prescriptive, evaluative, and obligatory dimension into social life" (Scott, 1995, 37). Practices that are consistent with and take into account the different assumptions and value systems of the national cultures are likely to be successful (Schneider, 1999). Cybercrimes are more justifiable in some societies compared to others. Blau (2004) describes how a Russian hacker-turned-teacher and his friends hacked programs and distributed them for free: "It was like our donation to society, it was a form of honor; [we were] like Robin Hood bringing programs to people". Similarly, many Indonesian hackers feel that cyber fraud is wrong but acceptable if the victim is from a developed country (see Box 2).

Elements of normative institutions also include trade associations or professional associations that can use social obligation requirements to induce certain behavior within the hacking community. For instance, the members of the Honker Union of China (also known as the Red Hackers) are required to behave according to the guidelines set by the organization. We propose that:

Proposition 2. *The rate of origin of online attacks in an economy is positively related to the existence of social norms that justify such attacks.*

4.5. Cognitive institutions

Cognitive institutions are associated with culture (Jepperson, 1991). These components represent culturally supported habits that influence hackers' behavior. In most cases, they are associated with

[12] For instance, the law enacted in Romania in 2003 punishes convicts with up to 15 years in prison (Romania Gateway, 2003).

[13] All propositions are stated on a ceteris paribusother things being equalbasis. The phrase ceteris paribus is implicit at the beginning of each proposition, and has not been explicitly stated.

cognitive legitimacy concerns that are based on subconsciously accepted rules and customs as well as some taken-for-granted cultural account of computer use (Berger and Luckmann, 1967). Scott (1995, 40) suggests that "cognitive elements constitute the nature of reality and the frames through which meaning is made". Cognitive programs affect the way people notice, categorize, and interpret stimuli from the environment. Although carried by individuals, cognitive programs are social in nature (Berger and Luckmann, 1967). Compliance in the case of cognitive legitimacy concerns is due to habits; hackers may not even be aware that they are complying.

4.6. Ideology[14]

Ideology is an important component of cognitive institutions that energizes the behavior of many computer hackers. A number of cyber attacks are linked with fights for ideology. Ideological hackers[15] attack websites to further political purposes. As it will become clear shortly, such hackings can be mapped with obligation/community-based intrinsic motivations.

While some ideological hackers express nationalistic longings (see next section and Box 3) by acting up in line with the government (de Kloet, 2002), others act against the nation-state where they live. For instance, in the mid-2001, Cyberjihad, a group of hackers in Indonesia attacked the Web site of the Indonesian police to force them to free a militant Muslim leader (Antariksa, 2001, p. 15). Similarly, in October 2001, a hacker in China replaced a Chinese government website with pornographic contents (de Kloet, 2002). In addition to nationalism and religion, hackers' interests are also framed by fight against global capitalism (de Kloet, 2002). Such hackers are likely to attack networks of big multinationals.

Box 3
Internet as a medium to express nationalistic and patriotic longings

Some scholars suggest that the Internet disconnects citizens from public life, while other studies have found that it provides a venue for further participation in public life (Weber et al., 2003). According to the latter camp, the Internet arguably is an important new venue for stimulating civic participation and engagement. In particular, the Internet has facilitated the expression of nationalistic and patriotic longings.

The Chinese nationalism and patriotism are the focus of this case. China's transition to market economy has followed a trajectory significantly different from those of Eastern Europe and the Soviet Union. While Russia followed the Western prescriptions, China has successfully blended nationalism with Marxism (Shlapentokh, 2002).

Before proceeding further, let us briefly review Chinese and American versions of nationalism and patriotism. Pei (2003) has identified several dimensions of nationalism. Consider two of them: source and bases. In terms

[14] Ideology is defined as the taken-for-granted assumptions, beliefs and value systems shared collectively by social groups (Simpson, 1993). The American Heritage Dictionary, third edition, defines ideology as "the body of ideas reflecting the social needs and aspirations of an individual, a group, a class, or a culture".

[15] Hacking (Beginner): Hackers Explained (PART I), www.linuxexposed.com/modules.php?op=modload&name=News&file=article&sid=528.

of source, he argues that some nationalism are product of grass-root voluntarism (as U.S. nationalism) while others are fostered by government elites and promoted by the apparatus of the state (police, military, state-run media). Chinese nationalism is viewed as state sponsored and an attempt to fill an "ideological vacuum" left by the weakening socialism (Oksenberg, 1997; Christensen, 1996; Sautman, 2001).

In terms of bases, Pei distinguishes nationalism related to universalistic ideals (democracy, rule of law, free marketplace) and institutions from that based on ethnicity, religion, language, and geography. China falls in the latter category. In China, the state arguably bolsters its legitimacy through invoking a deep sense of "Chineseness" among citizens (Ong, 1997; Barme, 1999; Hansen, 1999). Sautman (2001) has documented how China has adapted a body of complex scholarship to invoke a deep sense of "Chineseness". In a review of literature, Sautman (2001) concludes: "Nowhere is this more pronounced than in China, where these disciplines [Archaeology and paleoanthropology[16]] provide the conceptual warp and woof of China's "racial" nationalism".

Chinese hackers have expressed their patriotic and nationalistic longings in several cyber wars. In August 1999, Web defacements led to a cyber war between Chinese and Taiwanese hackers. Initially, Chinese hackers defaced several Taiwanese websites with pro-China messages and said that Taiwan was and would always be a part of China (Denning, 2000). Chinese have also fought cyber wars with Indonesians and Japanese (de Kloet, 2002).

The US–China cyber wars are particularly telling. In September 1999, following the accidental bombing of the Chinese Embassy in Belgrade, a group of hackers that identified itself as Level Seven Crew, defaced the Website of the U.S. embassy in China and replaced the home page with racist and anti-government slogans (Denning, 2000). Following the collision of a U.S. surveillance plane and a Chinese fighter in 2001, a Chinese hacking group publicly released its plans for a "Net War", which was planned to continue until the anniversary of the bombing in Belgrade (May 7). In response, hacking groups from the US, Brazil and Europe attacked Chinese websites. According to a *NewMax.com Wires* article (www.newsmax.com/archives/articles/2001/5/22/84452.shtml) Chinese hackers attacked about 1100 U.S. sites while American hackers broke into 1600 Chinese sites. Similarly, after the collision of a Chinese fighter jet with a U.S. surveillance plane in April 2001, Chinese hacking group attacked hundreds of U.S. Web sites including that of the White House (Bridis, 2001).

A comparative study between mailings of Chinese and Americans indicated that fierce feelings of nationalist fervor had fuelled both camps (Kluver, 2001, p. 7). On several American websites, Chinese left: "We are ready to devote anything to our motherland, including our lives" (Smith, 2001). The Chinese hackers involved in the attacks argued that they were patriotic and thus did not do anything wrong.

[16] Archaeology is the study of ancient societies and cultures. Paleoanthropology is the study of the human fossil record.

Hackings by Islamic activists are also interesting examples of ideological cyber attacks. Except for occasional India–Pakistan and Israel–Palestine cyber wars, hacking by Islamist activists was insignificant before September 11, 2001. *mi2g Intelligence Unit* reported increasing Islamist hacking, the targets being networks of the US, Britain, Australia and other coalition partners as well as domestic networks of Russia, Turkey, Indonesia, Pakistan, Saudi Arabia, Morocco and Kuwait.[17]

To take yet another example of ideological hacking, in June 1998, six hackers from the US, the UK, the Netherlands, and New Zealand (identifying themselves as *Milworm*) hacked the Web site of India's Bhabha Atomic Research Center (BARC) and left a message: "If a nuclear war does start, you will be the first to scream" (Denning, 2000). Similarly, in South Korea, 58 Internet servers were attacked by a Japanese student in November 2003 to protest the war in Iraq (Duk-kun, 2003).

Nationalism and patriotism[18,19] can be considered as conceptual subsets of ideology. These are universally accepted as vital elements of state strength (Alagappa, 1995, 26–7). Salmon (1995) argues that "patriotism or attachment to one's country often leads to actions and attitudes which are disinterested or self-sacrificing, help solve free-riding problems" (p. 296). We can find many instances of hackings linked to nationalism and patriotism. To take an example, in the early 1990s, a group of Portuguese hackers named TOXYN infiltrated a number of Indonesian government websites to fight against the occupation of East Timor (de Kloet, 2002). Indonesian hackers responded by attacking Portuguese servers that hosted the East Timor movement (Antariksa, 2001). To take another example, in 1997, cyber attacks occurred in Sri Lanka in support of the Tamil Tiger separatists. The strike was intended to disrupt government communications by overloading Sri Lankan embassies with millions of e-mails (Havely, 2000). To take yet another example, in 1998, Indian army's website on Kashmir was "hijacked" by supporters of Pakistan's claim to the disputed territory, who plastered the site with their own political slogans (Havely, 2000). In response, in July 2001, the website of the Pakistan based militant outfit Lashkar-e-Tayiba was attacked by a hacker who called himself 'True Indian' (Peer, 2001). It was in response to attacks of G-force, a Pakistani hacker group, to the Indian Ministry of External Affairs' websites.

Nationalism and patriotism were dominant codes of appeal in the US–China cyber wars of April–May 2001 (see Box 3). Quoting a security engineer from Guangdong Province of China, Netease[20] reported the daily number of attacks increased by over 20 times the average during April–May, 2001. Analyzing the US–China cyber wars, Kluver (2001, p. 8) concluded that "the technological optimism which sees in the Internet the end of nationalism and parochialism is an

[17] The rise of extremist hacking, criminal syndicates, http://star-techcentral.com/tech/story.asp?file=/2004/10/26/technology/9225925&sec=technology.

[18] Before proceeding further, it is important to review definitional issues and difference in the meanings of the two terms. One school of thought maintains that "there is a distinction, but no real difference" between patriotism and nationalism (Pei, 2003). According to this school, patriotism is related with "allegiance to one's country" and nationalism as "sentiments of ethno-national superiority" (Pei, 2003). Brown (1999) considers patriotism as identification with territory whereas nationalism as identification with the group. For the purpose of this paper, we use the terms nationalism and patriotism interchangeably.

[19] There are some studies that have compared the impacts of nationalism and patriotism on consumer behavior. In a comparative study of the impact of patriotism and nationalism on consumer ethnocentrism in Turkey and the Czech Republic, Balabanis et al. (2001) found that the impact of patriotism and nationalism on consumer ethnocentrism is not consistent across the two countries. Consumer ethnocentrism in Turkey is fueled by patriotism, and in the Czech Republic by nationalism.

[20] See http://news.163.com/editor/010501/010501_168631.html.

unrealistic understanding of how the Internet functions as a medium for human interaction". The next proposition is:

Proposition 3. *An organization's conflict of ideology with a hacking unit is likely to result in cyber attacks by the latter against the former.*

5. Stock of hacking skills relative to the availability of economic opportunities

Unlike conventional crimes against persons or property such as rape, burglary and murder, cybercrimes are very skill intensive. Stock of hacking skills is thus a prerequisite to online crimes. Whereas minimal skill is needed for opportunistic attacks, targeted attacks require more sophisticated skills.

Crime rates are, however, tightly linked to the lack of economic opportunities. Becker (1995, p. 10) comments on the increased number of crimes committed by teenagers: ... [L]ow earnings are a factor behind crime, and teenagers have lower earnings and fewer opportunities.

The combination of over-educated and under-employed computer experts has made Russia and some Eastern European countries fertile ground for hackers. In these counties, there are a large number of students good at mathematics, physics and computer science but having difficulties to find jobs (Blau, 2004). The situation was exacerbated by a financial crash in 1998 that left many computer programmers unemployed. A self-described hacker from Moscow told reporters: "Hacking is one of the few good jobs left here" (Walker, 2004). Regarding computer attacks originating from Romania, the US-based Internet Fraud Complaint Center, run by the FBI and the National White Collar Crime Center has reported: "Frustrated with the employment possibilities offered in Romania, some of the world's most talented computer students are exploiting their talents online" (Romania Gateway, 2003).

A large number of extortion related cyberattacks originate from Eastern Europe and Russia (see Box 1). These hackers possess capability to do very sophisticated attacks with limited computer power (Walker, 2004). It can be attributed to Russia's highly educated workforce and programming skills.[21] Russian hackers have a deep understanding of networks and know how to "get in and out without a trace" (Walker, 2004). The above leads to the following:

Proposition 4. *The rate of origin of online crimes in an economy is positively related to the stock of hacking skills relative to the availability of economic opportunities.*

6. Types of cyber attacks

Cyber attacks can be classified into two types: targeted and opportunistic attacks. In targeted attacks, specific tools are used against specific cyber targets. Opportunistic attacks, on the other hand, entail releasing worms and viruses that spread indiscriminately across the Internet. At this point, it must be emphasized that targeted attacks more dangerous than

[21] Hackers—the new breed of gangsters, August 3, 2004, http://newpaper.asia1.com.sg/top/story/0,4136,69503-1-1098892740,00.html.

opportunistic attacks and many of them have bigger financial ramifications. Moreover, the proportion of cyber attacks that are targeted is increasing over time.

Targeted attacks are carried out by skilled hackers with expertise to do serious damages. Some of them are motivated by financial gains (see Boxes 1 and 2). Targeted attacks are also initiated by terrorists, rival companies, ideological hackers or government agencies. The government of Burma, for instance, reportedly monitors online critics of the regime and sends them viruses attached in emails (Havely, 2000). Similarly, in August 2004, six hackers were convicted by a Californian court for their involvement in DoS attacks against business rivals (Leyden, 2004).

7. Motivation

A deeper understanding of web attacks requires an examination of motivation (Coates, 2002) that energizes the behavior of a hacking unit. The nature of web attacks allows us to draw an analogy with conventional wars. Just like in the physical world, wars on the web are fought for material ends as well as for intangible goals such as honor, dominance and prestige (Hirshleifer, 1998). Drawing from psychology and economics literature, we divide these motivations into two categories.

7.1. Intrinsic motivation

The theory of intrinsic motivation is based on the premise that human need for competence and self-determination are linked with interest and enjoyment (Deci and Ryan, 1985, 35). According to Ryan and Deci (2000), intrinsically motivated individuals do activities for "inherent satisfactions rather than for some separable consequence". They argue that "when intrinsically motivated, a person is moved to act for the fun or challenge entailed rather than because of external prods, pressures or rewards". Intrinsic motivation can be separated into two separate constituents: (1) enjoyment-based intrinsic motivation and (2) obligation/community-based intrinsic motivation (Lindenberg, 2001).

7.1.1. Enjoyment-based intrinsic motivation

Central to the concept of intrinsic motivation is having fun or enjoying oneself when taking part in an activity (Deci and Ryan, 1985). Csikszentmihalyi (1975), one of the first psychologists to study the enjoyment dimension, emphasized that some activities were pursued for the sake of enjoyment derived from doing them. Csikszentmihalyi refers it to a satisfying flow of activity. Shapira (1976) argues that this category of motivation is related with fulfilling a challenging task without an external reward. Maverick hackers, for instance, attack websites because of the perceived challenges and without any desire for financial incentives.

7.1.2. Obligation/community-based intrinsic motivation

Lindenberg (2001) argues that acting on the basis of principle is also a form of intrinsic motivation. He argues that individuals may be socialized into acting appropriately and in a manner consistent with the norms of a group. The goal to act consistently within the norms of a group can trigger a normative frame of action (Lakhani and Wolf, 2005). The group to which hackers associate themselves could be a nation, a territory, a terrorist organization or an association of hackers. The obligation/community goal is strongest when gain seeking (gaining personal advantage at the expense of other group members) by individuals within the reference community is minimized (Lakhani and Wolf, 2005).

7.2. Extrinsic motivation

Economists have contributed to our understanding of how extrinsic motivations drive human behavior. Economic theory suggests that human behavior is a result of "incentives applied from outside the person" (Frey, 1997, 13). The benefits accruing to the individual may be immediate or delayed. The amount of financial incentives and the amount of motivation driving a hacker's behavior co-vary positively. Extrinsically motivated hackers are thus likely to attack networks of companies with higher digitization of values (higher potential financial incentives). For instance, cyber extortionists target online casinos, banks, and e-commerce hubs. These attacks are carefully planned. After cracking into victims' computers systems, extortionists normally send e-mails demanding that ransoms as high as $100,000 be sent via money transfer agencies such as Western Union. Companies are threatened with sophisticated disruption of their computer systems if they do not comply. Although some victims reject demands for money and absorb cyber attack, other victims choose to pay (also see Box 1).

7.3. Combination of motivations

In many cases, human behavior is driven by multiple motivations—different forms of intrinsic and extrinsic (Lindenberg, 2001). Thus, a person who wants to make money and also have fun is likely to choose opportunities that give economic reward (ransom from hacking a e-commerce website) with a sense of having fun (Lakhani and Wolf, 2005). To take one example, the hackers protesting India's nuclear weapons tests in 1998 not only fought for ideology (community-based intrinsic motivation), but also admitted they attacked the website for thrills (enjoyment based intrinsic motivation) (Denning, 2000). The combination of motivations also changes over time. Blau (2004) quotes a Russian hacker: "There is more of a financial incentive [extrinsic motivation] now for hackers and crackers as well as for virus writers to write for money and not just for glory or some political motive [intrinsic motivation]".

8. Profile of target organization

8.1. Symbolic significance and criticalness

The ideal targets for terrorists of September 11, 2001 were the World Trade Center's Twin Towers, the White House and the Pentagon, the ones with tremendous symbolic significance (Coates, 2002). Hackers similarly have ideal targets. Attacks initiated by terrorists are likely to be targeted against decisive and critical infrastructure systems such as telecommunications, the supply of gas, oil and fuel (Comité Européen Des Assurances, 2004).

Following the collision of an American spy plane and a Chinese jet in April 2001, Chinese and U.S. hackers attacked each other's websites. Each camp selected websites that had symbolic values. In the US, the White House's site was shut down for many hours; there was a virus attack against computers at the California Department of Justice; and Ohio's Bellaire School District site played the Chinese national anthem displaying Chinese flag (Smith, 2001). In China, sina.com, one of the most popular portals; the website of Xinhua news agency; and those of local governments were attacked (The Happy Hacker, 2001). Thus, we propose that:

Proposition 5. *The symbolic significance and criticalness of a network increases its likelihood of being a cybercrime target.*

8.2. Digitization of value

Crimes target sources of value, and for this reason, digitization of value is tightly linked with digitization of crime.[22] Large companies have larger networks which offer more targets to hackers. A survey of Riptech indicated that attackers are more likely to launch targeted attacks against larger companies than smaller. Businesses with a high dependence on digital technologies–including online casinos, banks, and e-commerce hubs–are more likely to be the target (Kshetri, 2005) for extrinsically motivated hackers. For instance, estimates suggest that a few hours downtime on Super Bowl weekend cost online casinos up to $1 million (Onlinecasinonews.com, 2004). According to IDC, over 60% of computer hacks targeted financial institutions in 2003 (Swartz, 2004). Similarly, in the first half of 2004, 16% of e-commerce attacks were targeted compared to 4% in 2003 (Symantec, 2004). Thus:

Proposition 6. *The degree of digitization of value of an organization increases its likelihood being a cybercrime target.*

8.3. Weakness of defense mechanisms

Weakness of defense mechanism co-varies positively with the likelihood of an attack. In the conventional world, for instance, a female-headed household is positively related to the probability of being a crime target (Glaeser and Sacerdote, 1999). In the digital world, hackers in most cases take advantage of unfixed software holes. Due to weak defenses of most computer networks, it is difficult track origins of cyber attacks (Kong and Swartz, 2000). Based on the above, a final proposition pertaining to the likelihood of an organization's network being attacked is:

Proposition 7. *Weakness of defense mechanisms of a network is positively related to its likelihood of being a cybercrime target.*

9. Discussion and implications

This paper has contributed to the conceptual and empirical understanding of global cyber wars and crimes. The analyses of the paper indicated that the nature of the source of a web attack is a function of the nature of regulative, normative and cognitive legitimacy to the attacking unit; and stocks of hacking skills relative to the availability of economic opportunities. An attacking unit's selection criteria for the target include symbolic significance and degree of digitization of values. Extrinsically motivated hackers are likely to attack the networks with high degree of digitization of values. These include financial institutions, e-commerce hubs and online casinos. Intrinsically motivated hackers' targeted attacks, on the other hand, are directed towards organizations that with symbolic significance and criticalness. These include websites of government, critical infrastructures and also some companies that are perceived as national symbol. Different motivations of hackers, source characteristics and target country characteristics lead to different likelihoods of attacks on different organizations. Put differently, an independent variable may have different coefficients in regressions with attacks on different organizations as dependent variables.

[22] Bernard Clements, Laurent Beslay and Duncan Gilson, Cyber-Security Issues http://www.jrc.es/home/report/english/articles/vol57/EDI1E576.htm.

Table 2
Classification of targeted cyber attacks by national border: an illustration from the U.S. perspective

		Target	
		Domestic	Foreign
Source	Domestic	[1] • Former and current employees • Domestic customers • Domestic competitors • Domestic hackers • Domestic organized criminal groups (e.g., the "Phonemasters")	[3] • U.S. cyber scammers attacking foreign websites (e.g., ShadowCrew) • Patriotic/nationalistic hackers (e.g., those attacking Chinese websites) • Other ideological hackers (e.g., those attacking India's Bhabha Atomic Research Center)
	Foreign	[2] • Foreign competitors • Foreign customers targeting U.S. companies • Foreign cyber scammers targeting U.S. companies/Internet users • Foreign organized criminal groups (e.g., Russian online extortionists) targeting U.S. companies • Foreign government agencies (e.g., the government of Burma sending virus-attached emails to its critics residing in the US) • Foreign Patriotic/nationalistic hackers (e.g., Chinese attacking U.S. websites) • Foreign terrorists (e.g., request from Afghanistan to provide hacking services)	[4] • Attack on US-based MNCs' foreign websites. • Attack on the websites of U.S. diplomatic offices (e.g., The China based Level Seven Crew's attack on the website of the U.S. embassy in China)

Nations across the world differ widely on key elements represented in Fig. 1 and hence on domestic/foreign composition of sources and targets of cyber attacks as well as attackers' motivations. To illustrate from the U.S. perspective, in Table 2, we have classified targeted cyber attacks impacting the US by national border in terms of target and source.

This paper has important managerial implications. First, the global cybercrime landscape is moving toward a higher proportion of targeted attacks. All organizations, however, are not equally attractive cybercrime targets. Whereas symbolic significance and criticalness of a network attract intrinsically motivated cyber criminals, larger businesses and those with a high dependence on digital technologies are lucrative targets for hackers that work for money. It is thus important for firms to assess the risks of their networks being cybercrime targets and devise appropriate defense mechanisms.

Second, like other technologies, deployment of defense mechanisms tends to diffuse from large to small organizations. This is commonly known as the *rank effect* in economics literature (Gotz, 1999). As large companies put stronger defense mechanisms against cyberattacks, small and medium size enterprises (SMEs) are more likely to become cybercrime targets. The proportion of total cybercrimes that target SMEs is thus likely to increase.

Third, cybercrimes are among the most underreported forms of criminality. Experts say less than 10% of cybercrimes are reported to authorities (Bednarz, 2004). In the conventional world, research has indicated that time taken to report a crime is one of the most important factors in

Table 3
Measuring the cyber safety environment

Stage of cyber safety	Institutional indicators	Business-related indicators
Number of attacks per 1000 Internet users.	Existence of laws that require appropriate defense mechanisms (+).	Proportion of revenue spent in network security (+).
Proportion of cyber attacks that are targeted.	Existence of laws that require reporting cybercrime (+).	Degree of compliance with cyber-criminals' demands (e.g., extortion money paid annually) (−).
	Proportion of reported crimes that are investigated (+). Proportion of reported crimes that lead to arrest (+). Proportion of reported crimes that lead to conviction (+). Severity of punishment for convicted cyber criminals (+). Existence of social norms that justify cyber attacks (−).	Willingness of cybercrime victims to report crimes (+).

+: positive contribution to cyber safety; −: negative contribution to cyber safety.

determining the probability of arrest (National Institute of Justice, 2001). Timely reporting of cyberattacks to authorities is thus likely to strengthen the rules of law and help combat cyber threats in the long run.

Fourth, some companies have set a dangerous precedent of negotiating with web terrorists by paying ransoms. Estimates suggest that gambling sites alone have paid millions of dollars to cyber extortionists annually. Ransom money sends positive cognitive messages and will fuel further cyberattacks by making criminals more sophisticated and organized. As criminals' skill, organization and intelligence co-vary positively with the odds of getting away with crimes (National Center for Policy Analysis, 2002), paying ransom contributes to the vicious circle of cybercrimes.

This paper also has several policy implications. First, there is no pure technological fix for security related problems involving technologies (Carblanc and Moers, 2003, Skolnikoff, 1989). Cooperation and collaboration among national governments, computer crime authorities and businesses are critical to combat cyber attacks. If national governments work with one another as well as with business communities to modify institutions by defining appropriate policies for the security of the digital world, it will result in lower transaction costs. Some signs of success have materialized,[23] but nations have very far to go before they can achieve even a moderate level of success. For instance, although Russia has signed agreements to help the US in investigating some crimes, computer crimes are not among them (Lemos, 2001). In 2001, the U.S. Department of Justice requested the assistance of Russian authorities but received no response (Lemos, 2001).

Second, enacting laws that require organizations to deploy appropriate defense mechanisms and making reporting of cybercrimes mandatory can help combat such crimes. U.S. government, for instance, requires commercial banks to secure their networks. The *Patriot Act* and the

[23] To take an example, Interpol played a critical role to catch a member of Cyber Lords in Japan. To take another example, over 60 Romanian hackers were arrested in joint operations involving the FBI, Secret Service, Scotland Yard, the U.S. Postal Inspection Service and a number of European police agencies (Romania Gateway, 2003). To take yet another example, in July 2004, collaboration between British and Russian police led to the arrest of the members of an online extortion ring accused of blackmailing online sports betting websites that cost British companies $120 million (sophos.com, 2004).

Gramm Leach Bliley (GLB) Act require new security measures including customer identification and privacy protection. Despite the existence of similar regulations for decades, *the Patriot Act* reflected a change in the U.S. banking landscape. Since the mid-2004, South Korea's National Cyber Security Center has mandated that all Internet-related hacking incidents must be reported (Ho, 2004). Many countries, however, do not have such laws.

Third, many countries are changing the regulative landscape towards severity of punishment. For instance, the *U.S. Patriot Act* brought cyber attacks into the definition of terrorism with penalties of up to 20 years in prison. The probability of arrest in cybercrimes is, however, very low since conventional law enforcement authorities lack skills required in dealing with such crimes. The severity of punishment is important, but what is still more critical in enhancing cyber safety is the certainty of punishment (Becker, 1995). The probability of arrest is likely to increase with more investments in the development of law enforcement capabilities.

Fourth, many small and poor countries lack resources to investigate cybercrimes (see Box 2). Big and rich nations' assistance to these countries, especially those with high rates of origin of cybercrimes, is urgently needed to combat global cyber threats originating from these countries.

Finally, various components of institutions, despite their connotation of persistence (Parto, 2005), durability (Hodgson, 2003) and stability (Scott, 2001, p.48), are subject to change in evolutionary time (Parto, 2005). Zucker (1988, p. 26) draws an analogy from physics to describe institutional change mechanisms. He argues that institutions continuously undergo change due to entropy, a tendency toward disorder or disorganization (p. 26). An implication of the entropy-like characteristics is that people can modify and reproduce (Scott, 2001) institutions. Managers and governmental officials thus can singly or cooperatively eliminate or at least minimize institutional forces that promote deviant cyber behavior.[24] In addition to enacting new laws to minimize cyber threats (change in regulative institutions), they can devise strategy to change social norms (change in normative institutions) that influence hackers' behavior.

An important area of future research concerns operationalizing the constructs discussed in this paper and testing the model presented in Fig. 1. Two possible approaches can be employed for this purpose. The first approach entails testing the model based on country-level data. Although Fig. 1 employs different levels of analysis, sources and target characteristics can be aggregated at the country level. For this purpose, Table 3 provides some measures of cyber safety and a non-exhaustive list of factors that reflect and determine the cyber safety environment.

The second approach is to apply economics of crimes to test the influence of characteristics of the source nation on hackers' willingness to commit cybercrimes. Following the economic approach, a cyber criminal weighs benefits and costs to make decision about engaging in a crime. A cybercrime is thus committed if the sum of perceived monetary benefits and perceived psychic benefits exceeds perceived psychic costs of committing a cybercrime plus the expected penalty effect (which is the product of the probability of arrests, the probability of conviction and perceived monetary opportunity costs of conviction) (Probasco and Davis, 1995). Surveys consisting of impacts of regulative, normative and cognitive institutions; and availability of economic opportunities on hackers' assessment of perceived cost–benefit of

[24] The author thanks a JIM reviewer for suggesting this point.

cybercrimes can be employed to test the model presented in Fig. 1. Respondents could be hackers and/or computer network experts from a number of countries. Similarly, surveys can also be conducted to predict profiles of target organization that different categories of hackers consider worthwhile to attack.

Preliminary evidence discussed in this paper indicates the shift in hackers' motivations from intrinsic to extrinsic. In this regard, another fruitful avenue for future research is to understand the determinants of the turning point. In-depth interviews with extrinsically motivated hackers would help understand how institutional and economic factors discussed in this paper transform motivations of attacking computer networks.

As mentioned above, all companies do not report attacks on their networks. Additional research is also needed to identify the determinants of self-selection bias in the reporting of cyber attacks. What factors distinguish firms that report attacks on their networks from those that do not? Are there international variations in the reporting patterns?

Acknowledgement

The author is grateful to the Temple University CIBER for its financial support to present an earlier version of this paper at the 6th Annual International Business Research Forum. Constructive feedbacks of the JIM editor, three anonymous reviewers and participants of the forum drastically improved the quality of the paper.

References

Adams, J., 2001. Virtual defense. Foreign Affairs, 98–112 (May/Jun).

Alagappa, M., 1995. Political Legitimacy in Southeast Asia. Stanford University Press, Stanford, CA.

Antariksa, 2001. I am a thief, not a hacker: Indonesia's electronic underground. Latitudes Magazine, 12–17 (July).

Balabanis, G., Diamantopoulos, A., Mueller, R.D., Melewar, T.C., 2001. The impact of nationalism, patriotism and internationalism on consumer ethnocentric tendencies. Journal of International Business Studies 32 (1), 157–175.

Barme, G., 1999. In the Red: On Contemporary Chinese Culture. Columbia University Press, New York.

Becker, G.S., 1995. The economics of crime. Cross Sections, Fall, 8–15. http://www.rich.frb.org/pubs/cross/crime/crime.pdf.

Bednarz, A., 2004. Profiling cybercriminals: a promising but immature science. Network World, November 29, http://www.nwfusion.com/supp/2004/cybercrime/112904profile.html?page=2.

Berger, P.L., Luckmann, T., 1967. The Social Construction of Reality: A Treatise in the Sociology of Knowledge. Doubleday, New York.

Blau, J., 2004. Viruses: from Russia, with love? IDG News Service, May 28. http://www.pcworld.com/news/article/0,aid,116304,00.asp.

Bridis, T., 2001. E-Espionage rekindles cold-war tensions—U.S. tries to identify hackers; millions of documents are stolen. Wall Street Journal, A.18 (Jun 27).

Brown, LC., 1999. The multiple identities of the Middle East. Foreign Affairs 78 (6), 158–159.

Carblanc, A., Moers, S., 2003. Towards a culture of online security. The OECD Observer, 30 (December).

Christensen, T., 1996. Chinese Realpolitik. Foreign Affairs 75 (5), 37–52.

Coates, J.F., 2002. What's next? Foreseeable terrorist acts. The Futurist 36 (5), 23–26.

CNN.Com., 2000. Rebuffed Internet extortionist posts stolen credit card data, January 10. http://cnn.com/2000/TECH/computing/01/10/credit.card.crack.2/index.html.

Comité Européen Des Assurances, 2004. Terrorist acts against computer installations and the role of the Internet in the context of International Terrorism Property Insurance Committee, IT Risks Insurance Sub-committee, February 2004. http://www.cea.assur.org/cea/v1.1/actu/pdf/uk/annexe180.pdf.

Csikszentmihalyi, M., 1975. Beyond Boredom and Anxiety: The Experience of Play in Work and Games. Jossey-Bass, San Francisco.

Darmosumarto, S., 2003. Battle on Internet credit card fraud still long, The Jakarta Post, December 08. http://www.crime-research.org/news/2003/12/Mess0802.html.
Deci, E.L, Ryan, R.M., 1985. Intrinsic Motivation and Self-determination in Human Behavior. Plenum Press, New York, NY.
de Kloet, J., 2002. Digitisation and its Asian discontents: the Internet, politics and hacking in China and Indonesia, First Monday, 7(9). URL: http://firstmonday.org/issues/issue7_9/kloet/index.html.
Deloitte Touche Tohmatsu, 2002. Australian Computer Crime and Security Survey. http://www.4law.co.il/346.pdf.
Denning, D.E., 2000. Hacktivism: an emerging threat to diplomacy, American Foreign Service Association. www.afsa.org/fsj/sept00/Denning.cfm.
Duk-kun, B., 2003. Largest Internet hacking ring uncovered. The Korea Times, 19 (November).
Foreign Policy, 2005. Caught in the Net: Australian Teens, p. 92. March/April.
Forensic Accounting Review and Computer Security Digest, 2001. FBI warns of Russian hackers stealing U.S. credit-card data, 17(8), 2.
Frey, B., 1997. Not Just for the Money: An Economic Theory of Brookfield. Edward Elgar Publishing Company, VT.
Glaeser, E.L., Sacerdote, B., 1999. Why is there more crime in cities? The Journal of Political Economy 107 (6), S225–S258 (Part 2).
Gomes, L., Bridis, T., 2001. FBI warns of Russian hackers stealing credit-card data from U.S. computers. Wall Street Journal, A.4 (March 9).
Gotz, G., 1999. Monopolistic competition and the diffusion of new technology. The Rand Journal of Economics 30 (4), 679–693.
Grow, B., Bush, J., 2005. Hacker hunters. Business Week (May 30).
Handelman, S., 1999. Russia's rule by racketeers. Wall Street Journal, A.28 (September 20).
Hansen, M., 1999. Lessons in Being Chinese: Minority Education and Ethnic Identity in Southwest China. University of Washington Press, Seattle.
Havely, J., 2000. Online's when states go to cyber-war. BBC News Wednesday, 16 February.
Hirshleifer, J., 1998. The bioeconomic causes of war. Managerial and Decision Economics 19 (7/8), 457–466.
Ho, S., 2004. Haven for hackers. Foreign Policy (November/December).
Hodgson, G.M., 2003. The hidden persuaders: institutions and individuals in economic theory. Cambridge Journal of Economics 27, 159–175.
Jepperson, R., 1991. Institutions, institutional effects, and institutionalism. In: Powell, W.W., DiMaggio, P.J. (Eds.), The New Institutionalism in Organizational Analysis. University of Chicago, Chicago, pp. 143–163.
Kluver, R., 2001. New media and the end of nationalism: China and the US in a war of words, *Mots Pluriels*, at www.arts.uwa.edu.au/MotsPluriels/MP1801ak.html, accessed 12 December 2001.
Kong, D., Swartz, J., 2000. Experts see rush of hack attacks coming. Recent costly hits show 'more brazen' criminals preying on companies. USA Today, September 27, p. 01.B.
Kshetri, N., 2005. Hacking the odds. Foreign Policy, 93 (May/June).
Lakhani, K.R., Wolf, R.G., 2005. In: Feller, J., Fitzgerald, B., Hissam, S., Lakhani, K.R. (Eds.), Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects Perspectives on Free and Open Source Software (2005). MIT Press.
Lemos, R., 2001. FBI "hack" raises global security concerns May 1, CNet News, http://news.com.com/2100-1001-950719.html.
Leyden, J., 2004. US credit card firm fights DDoS attack, 23 September, http://www.theregister.co.uk/2004/09/23/authorize_ddos_attack/.
Lieberman, D., 2003. Feds enlist hacker to foil piracy rings; plea agreement includes help in satellite TV cases. USA Today, B.01. (January 10).
Lim, M., 2001. From real to virtual (and back again): civil society, public sphere, and the Internet in Indonesia, Paper presented at Internet political economy forum conference Singapore.
Lindenberg, S., 2001. Intrinsic motivation in a new light. Kyklos 54 (2/3), 317–342.
Lorek, L., 2001. Russian Mafia Net Threat, Interactive Week, July 16, p. 11.
Lunev, S., 2001. 'Red Mafia' operating in the U.S.—helping terrorists, October 1, 2001, http://www.newsmax.com/archives/articles/2001/9/28/90942.shtml.
National Center for Policy Analysis 2002. Crime and punishment in Texas: update, http://www.ncpa.org/pub/st/st202/st202c.html.
National Institute of Justice, 2001. 2000 Annual Report to Congress, August 2001, http://www.ncjrs.org/txtfiles1/nij/189105.txt.

North, D.C., 1990. Institutions, Institutional Change and Economic Performance Cambridge. Cambridge University Press, UK.
Oksenberg, M., 1987. China's confident nationalism. Foreign Affairs 65 (3), 501–523.
Olson, M., 1965. The Logic of Collective Action: Public Goods and the Theory of Groups. Harvard University Press, Cambridge, MA.
Ong, A., 1997. Chinese modernities: narratives of nation and of capitalism. In: Ong, A., Nonini, D. (Eds.), Underground Empires: The Cultural Politics of Modern Chinese Transformation. Routledge, New York.
Onlinecasinonews.com, 2004. Mob's extortion attempt on Internet bookies, February 3, http://www.onlinecasinonews.com/ocnv2_1/article/article.asp?id=4748.
Oxley, J.E., Yeung, B., 2001. E-commerce readiness: institutional environment and international competitiveness. Journal of International Business Studies 32 (4), 705–723.
Parto, S., 2005. Economic activity and institutions: taking stock. Journal of Economic Issues 39 (1), 21–52.
Peer, B., 2001. Lashkar web site hacked, July 10, http://www.rediff.com/news/2001/jul/10hack1.htm.
Pei, M., 2003. The paradoxes of American nationalism. Foreign Policy 136, 30–37.
Porter, M.E., 2001. Strategy and the Internet. Harvard Business Review 79 (3), 63–78.
Probasco, JR., Davis, W.L., 1995. A human capital perspective on criminal careers. Journal of Applied Business Research 11 (3), 58–64.
Richmond, R., 2003. Selling strategies—scammed! Web merchants use new tools to keep buyers from ripping them off. Wall Street Journal, R.6 (Jan 27).
Riptech, 2002. Riptech Internet Security Threat Report, vol II, July 2002. http://www.4law.co.il/276.pdf.
Rogers, E.M., 1983. The Diffusion of Innovations, 3rd ed. Free Press, New York.
Romania Gateway. 2003. Romania emerges as nexus of cybercrime, October 24, http://ro-gateway.ro/node/185929/comnews/item?item_id=223937.
Rosenau, J.N., 1995. Security in a turbulent world. Current History 94 (592), 193–200.
Ryan, R.M., Deci, E.L., 2000. Self-determination theory and the facilitation of intrinsic motivation, social development, and well being. American Psychologist 55, 68–78.
Salmon, P., 1995. Nations competing against themselves: an interpretation of European integration. In: Breton, Galeotti, Salmon, Wintrobe (Eds.), Nationalism and Rationality. Cambridge University Press, Cambridge.
Sautman, B., 2001. Peking man and the politics of paleoanthropological nationalism in China. The Journal of Asian Studies 60 (1), 95–124.
Schneider, A., 1999. US neo-conservatism: cohort and cross-cultural perspective. The International Journal of Sociology and Social Policy 19 (12), 56–86.
Scott, R., 1995. Institutions and Organizations. Thousand Oaks, CA: Sage.
Scott, R., 2001. Institutions and Organizations. Thousand Oaks, CA: Sage.
Shapira, Z., 1976. Expectancy determinants of intrinsically motivated behavior. Journal of Personality and Social Psychology 34, 1235–1244.
Simpson, P., 1993. Language, Ideology and Point of View. Routledge, London.
Skolnikoff, E.B., 1989. Technology and the world tomorrow. Current History 88 (534), 5–13.
Shlapentokh, D., 2002. Post-Mao China: an alternative to 'The end of history'? Communist and Post-communist studies. Kidlington 35 (3), 237.
Shubert, A., 2003. Taking a swipe at cyber card fraud, CNN.com, February fs6, 2003, http://www.cnn.com/2003/WORLD/asiapcf/southeast/02/06/indonesia.fraud/.
Smith, C.S., 2001. The first world hacker war. New York Times, 4.2 (May 13).
sophos.com, 2004. Police crack suspected online extortion ring, Sophos reports, 23 July. http://www.sophos.com/virusinfo/articles/extortion.html.
Swartz, J., Crooks slither into Net's shady nooks and crannies crime explodes as legions of strong-arm thugs, sneaky thieves log on USA Today, October 21, www.usatoday.com/printedition/money/20041021/cybercrimecover.art.htm.
Sullivan, B., 2004. Foreign fraud hits U.S. e-commerce firms hard, MSNBC, April 1, http://www.msnbc.msn.com/id/4648378/.
Symantec., 2004. Symantec Internet Security Threat Report, vol. VI. http://www.4law.co.il/L138.pdf.
Tedjasukmana, J., 2002. The no-payment plan: thousands of young Indonesians commit cyberfraud for fun and profit, September 23, 2002, http://www.time.com/time/globalbusiness/article/0,9171,1101020923-351237,00.html.
The Economist, 2003. Special report: fighting the worms of mass destruction—Internet security; November 29, 101.
The Happy Hacker, 2001. The US/China cyberwar of April/May 2001, http://www.happyhacker.org/news/china.shtml, accessed 14 November 2001.
Varese, F., 2002. The Russian Mafia: Private Protection in a New Market Economy. Oxford University Press, New York.

Verton, D., 2002. FBI chief: Lack of incident reporting slows cybercrime fight October 31 Computerworld, http://computerworld.com/securitytopics/security/cybercrime/story/0,10801,75532,00.html.

Walker, C., 2004. Russian mafia extorts gambling websites June, http://www.americanmafia.com/cgi/clickcount.pl?url=www.americanmafia.com/Feature_Articles_270.html.

Weber, L.M., Loumakis, A., Bergman, J., 2003. Who participates and why?: an analysis of citizens on the Internet and the mass public. Social Science Computer Review 21 (1), 26–42.

Williams, P. 2001. Organized crime and cybercrime: synergies, trends, and responses, 13 August, Office of International Information Programs, U.S. Department of State, http://usinfo.state.gov.

Williamson, O.E., 1975. Markets and Hierarchies: Analysis and Antitrust Implications. Free Press, New York.

Zucker, L.G., 1988. Where do institutional patterns come from? Organizations as actors in social systems. In: Zucker, L.G. (Ed.), Institutional Patterns and Organizations: Culture and Environment. Ballinger, Cambridge, MA, pp. 23–49.