Chapter 7
Global Heterogeneity in the Pattern of the Cybercrime Industry

Why should an Indonesian get arrested for damaging [an] American business? (an Indonesian hacker, cf. Shubert, 2003).

"We are ready to devote anything to our motherland, including our lives," message left by Chinese hackers on several American websites in a 2001 cyber war with American hackers (cf. Smith, 2001).

Abstract This chapter draws upon literatures on psychology, economics, international relation, and warfare to propose a framework to explain international heterogeneity in cybercrimes. 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.

7.1 Introduction

Information and communications technologies (ICTs) have drastically increased the porosity among national borders and contributed to the growth of transnational organized crimes and an illicit global economy (Etges & Sutcliffe, 2008; Naím, 2005; Rosenau, 1995; Serio & Gorkin, 2003). The increased porosity and anonymity of the Internet have superimposed in a complex interaction that has enabled criminal and violent groups, transnational terrorist organizations, and companies engaged in espionage to expand their operations globally. Government-backed cyberwarfare in some countries (Comité Européen Des Assurances, 2004) and maverick hackers testing their skills have further threatened the security of the digital world. Commenting on a rapid rise of cybercrimes, McAfee analyst Greg Day notes, "Blackmail, money motivation and new opportunities cross international borders" (Muncaster, 2006). Hi-tech and cybercrimes are among Interpol's top six priorities

N. Kshetri, *The Global Cybercrime Industry*, DOI 10.1007/978-3-642-11522-6_7,

(drugs and criminal organizations, tracking fugitives, public safety and terrorism, trafficking of human beings, and corruption are the other five) (Interpol, 2007).

Steffensmeier and Ulmer (2006) note, "the concept of criminal entrepreneurship ... implies that some groups are better endowed to exploit opportunities for illegal gain, whereas other groups may be weakly positioned to do so." Extending this line of reasoning at the institutional level, we can argue that institutions in some societies are likely to provide better payoffs and less political risk to cyber-criminals than others.

7.2 The Global Digital Security Threat: A Brief Survey

A large proportion of cyberattacks are international in scope (Tables 7.1 and 7.2). According to a report released by the FBI in January 2006, the agency tracked cyberattacks targeting the United States from 36 different countries (Regan, 2006). A 2002 survey of Australian firms indicated that 24% respondents perceived foreign governments as sources of attacks and 30% perceived foreign companies as such sources (Deloitte Touche Tohmatsu, 2002). In October 2009, largest Australian

Table 7.1 Top cybercrime sources (2002–2004)

Countries from which most online fraud originates[a]	Rank of countries according to percent of orders that US 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	Former Yugoslavia	Latvia	Kuwait (50.8)	USA (40)
Indonesia	Nigeria	Macau	Israel (33.1)	Germany (7.6)
Former 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).

Table 7.2 Top cybercrime sources (2007)

Top infection program creating countries in (2007)[a]	Top ten malware-hosting countries in (2007)[b]	Malicious activity per broadband user (second-half of 2007)[c]	Top ten countries for spam origin (second-half of 2007)[c]	Top countries hosting phishing websites (second-half of 2007)[c]	Top countries by perpetrators based on complaints made to I3C (second-half of 2007)[d]
The United States (35%)	China (51.4%)	Peru (9%)	The United States (40%)	The United States (66%)	The United States (63.2%)
China (30%)	The United States (23.4%)	The United States (7%)	The United Kingdom (5%)	China (14%)	The United Kingdom (15.3%)
Brazil (14.2%)	Russia (9.6%)	Poland (6%)	Russia (4%)	Romania (5%)	Nigeria (5.7%)
Russia (4.1%)	Ukraine (3.0%)	Argentina (6%)	China (4%)	Guam (5%)	Canada (5.6%)
Sweden (3.8%)	Germany (2.3%)	Israel (6%)	Poland (3%)	France (5%)	Romania (1.5%)
Ukraine (3.4%)	Poland (0.9%)	India (5%)	Taiwan (3%)	German (1%)	Italy (1.3%)
The United Kingdom and India Combined (1.3%)[e]	The United Kingdom (0.7%)	Taiwan (5%)	Japan (3%)	Italy (1%)	Spain (0.9%)
Germany (1%)	France (0.7%)	Chile (5%)	Germany (3%)	Canada (1%)	South Africa (0.9%)
	Canada (0.7%)	Canada (5%)	South Korea (3%)	Sweden (1%)	Russia (0.8%)
	Netherlands (0.7%)	Sweden (4%)	Spain (2%)	Netherlands (1%)	Ghana (0.7%)

[a]Greenberg (2007).
[b]sophos.com (2008).
[c]Symantec Internet Security Threat Report Vol. XIII, 2008.
[d]Internet Crime Complaint Center (2007) 2007 Internet Crime Report, http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf
[e]Sophos' list. Both countries use British English. Sophos researchers could not be separate the countries but thought that the majority of that criminal activity came from the UK.

banks' representatives told a senate inquiry into cybercrime that 70% of phishing attacks to their customers originated outside Australia (Winterford, 2009).

The United States is the No. 1 country in terms of source as well as targets for web attacks. According to a *Foreign Policy* article (March/April, 2008), 61% of the world's DoS attacks targeted US-based computers. Likewise, one estimate suggested that 66.1% of Internet frauds occur in the United States (Datamonitor, 2009). Many cyber-criminals targeting US businesses and consumers operate outside of US jurisdiction (Grow & Bush, 2005; Hahn & Layne-Farrar, 2006).

The US share in the global cybercrime industry is decreasing rapidly. The proportion of attacks originated from the United States dropped from 58% in the second-half of 2003 to 37% in the first-half of 2004 (Symantec, 2004).

As noted in Chap. 1, a large number of cybercrimes result from international collaborations. A hacker accused of pirating DirecTV and EchoStar signals in Florida told law-enforcement authorities that he had 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 United States in the mid-2005, had 4,000 members in a number of countries including Bulgaria, Canada, Poland, Sweden, and the United States (Grow & Bush, 2005). Mohammad Khairuddin Abdullah, Malaysia's HeiTech Padu Berhad's director noted that Russian mafia and Japanese Yakuza have financially sponsored the country's cyber-criminals (Ismail, 2008).

Tables 7.1 and 7.2 rank the world's top nations in terms of cyberattacks and frauds on the Internet. One estimate suggests that in 2003, less than 1% of computer attacks originate in countries that the United States considers "breeding grounds for terrorists" (The Economist, 2003). Another estimate suggests that 60% of fraudulent transactions originate from just 15 nations (Table 7.1).

7.3 Pattern of the Global Cyber-War and Crime: A Proposed Model

Our proposed model on the pattern of global cyberattacks is presented in Fig. 7.1. 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.

7.3.1 Characteristics of the Source Nation

7.3.1.1 Regulative Institutions: Strength of the Rule of Law

An issue that deserves mention relates to regulatory arbitrage. Economies worldwide vary greatly in terms of the legal systems related to cybercrimes. Moreover, legal systems take long time to change (Dempsey, 2008).

Prior research indicates that criminals avoid prosecution by using "clever regulatory arbitrage" (Levi, 2002, p. 905). Cyberattacks have tremendously benefited from

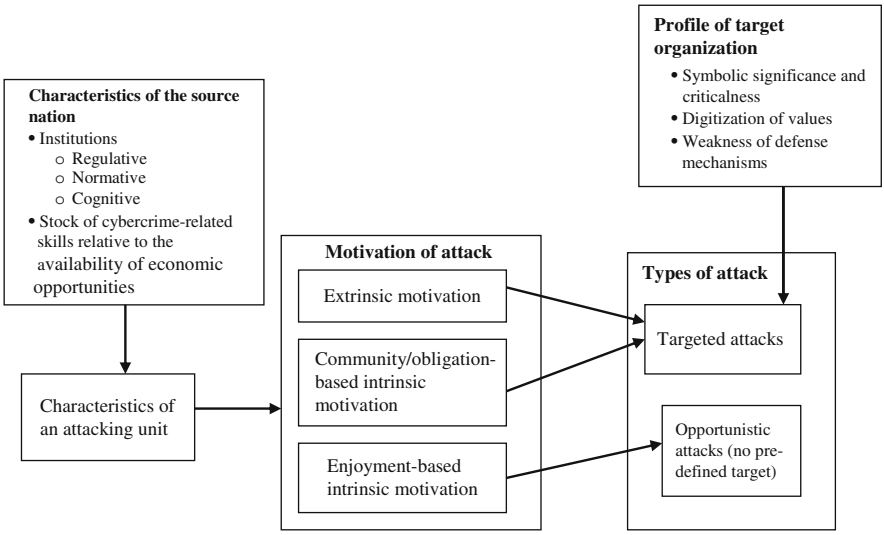

Fig. 7.1 Understanding the pattern of the global cyberattacks: a proposed framework

jurisdictional arbitrage. The lack of a strong rule of law is associated with the origination of cyberattacks (see Boxes 7.1 and 7.2). Not surprisingly, many organized cybercrimes are initiated from countries that have few or no laws directed against cybercrimes and little capacity and willingness to enforce existing laws (Grow & Bush, 2005; Williams, 2001; see Tables 7.1 and 7.2).

Box 7.1 Internet-led Globalization of Russian Organized Crime Group

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.

The Mafia and 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. In recent years, the Russian Mafia has developed expertise in cybercrime (Giannangeli, 2008).

Mafia groups have developed 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[4] on Worldpay[5] System that affected thousands of online casinos.

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 US 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 US 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 & 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.

The Cybercrime Workforce

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. Eighty-two percent of respondents participating in a worldwide poll conducted on a hacker-oriented website indicated that Russia had the world's best computer hackers. Only 5% of the respondents believed that American hackers were the best[6] (Walker, 2004).

Formal Institutions and Cybercrimes

The fragile property rights, too weak state (Varese, 2002), inefficient police, 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). The police said most hackers are young and educated, work independently, and do not fit police profiles of criminals (Newpaper.asia1.com.sg, 2004).

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

Box 7.2 Indonesia's Electronic Underground

Pervasive Credit Card Fraud in Indonesia

Credit card fraud has been pervasive in Indonesia. Estimates suggested that over 20% of Internet credit card transactions in Indonesia were fraudulent (Tedjasukmana, 2002), which were valued at $6 million a year in the early 2000s (Darmosumarto, 2003). Indonesian police also believed that the 2002 terrorist bombings in Bali were financed through online credit card fraud (GAO Reports June 22, 2007).

Users of stolen credit card information (known as carders) buy a wide range of items on the Internet from foreign countries. Warnets, the Indonesian 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).

An annual survey of *CyberSource Corp*. released in 2006 ranked Indonesia as the world's third riskiest country for online transactions, only behind

Nigeria and China (Lindenmayer, 2006). Indonesia has been consistently rated among the top nations in terms of fraudulent activities on the Internet (Table 7.1). The US online merchants consider Indonesia as one of the high-risk countries and block 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).

Cognitive Acceptance of Cyber-Fraud

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[7] 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).

Weak Regulative Institutions to Fight Cybercrimes

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). The lack of resources such as manpower, equipment, and funding has been a serious problem. Only 15% of reported incidents are actually investigated (Shubert, 2003). Indonesia's Information Technology Sub-Directorate of the Directorate of Special Crimes of the National Police Headquarters had only one dial-up connection in 2002.

In 2003, the Indonesian government submitted to the parliament a draft Cyber Law on information technology, electronic transactions, and freedom of information on the Internet. Progress on the law, however, has been slow (The Economist Intelligence Unit Limited, 2008). A special committee was formed to evaluate the law in November 2004. The bill was resubmitted in July 2005. In March 2008, the parliament finally approved the proposed draft Cyber Law (Handayani, 2008).

Regulative institutions dealing with cybercrimes are non-existent at worst and thin at best in developing countries. Many developing economies lack regulative framework to fight cybercrimes. For instance, as of the mid-2009, Asian

economies such as Laos Cambodia and Vietnam had no cybercrime laws (Kirk, 2009). Likewise, as of September 2009, some countries in Africa and the Middle East such as Iraq, Morocco, Tunisia, and Egypt did not have such legislations (Ryan, 2009).

Many developing economies such as those in Eastern Europe and Russia have weak cybercrime laws and a lack of enforcement mechanisms, which have provided a fertile ground for computer crimes (see Box 7.1 for Russia). Many activities that are considered illegal in the United States and Western Europe have not been outlawed in these countries.

The Russian Business Network (RBN) reportedly sold website hosting services to cyber-criminal. Krebs (2007) quoted an analyst with Kaspersky Lab, a Russian anti-virus and computer security firm: "They make money on the services they provide ... the illegal activities are all carried out by groups that buy hosting services ....RBN, ... does not violate the law. From a legal point of view, they are clean." According to the Serious Organised Crime Agency (Soca), the RBN allegedly bribed local police, judges, and government officials (cf. Leyden, 2009). An *Economist.com* article (2007) noted

> Despite the attention it is receiving from Western law enforcement agencies, RBN is not on the run. Its users are becoming more sophisticated, moving for example from simple phishing (using fake e-mails) to malware known as "trojans" that sit inside a victim's computer collecting passwords and other sensitive information and sending them to their criminal masters.

David Pérez, a consultant to Spanish banks, noted that among about hundred illegal servers, he identified, he could break into only three because many were located in Russia. The problem was further compounded as server administrators were often in yet another country (Sutherland, 2008).

A related point is that in most cases, it is difficult to decide which jurisdiction should rule on a cybercrime case. Once jurisdiction is determined, extradition may prove to be a challenge of another magnitude. For instance, to extradite from a county, the US law requires the existence of an extradition treaty with the country. In addition, the treaty must either list the specific crimes covered by it, or require dual criminality, that is, the US law is recognized in the country (Godoy, 2000). There has been an absence of international agreement on what constitutes a cybercriminal activity (Jewkes & Andrews, 2005). The United States has signed Mutual Legal Assistance Treaties with only a few nations (Katyal, 2001). As of 2000, the United States had about 100 extradition treaties (Gabrys, 2002).

In some countries, it is unconstitutional to extradite citizens even if they are engaged in criminal activities. For instance, according to article 25 of the Constitution of Ukraine, a citizen of the country "cannot be expelled from Ukraine or extradited to other state" (ohchr.org, 2007).

If a country does not outlaw a computer crime, the dual criminality doctrine prevents extradition (Katyal, 2001). Perhaps the best example of this is the 1992 Swiss hackers' attack on the San Diego Supercomputer center. The Swiss government did not cooperate with US authorities because of dual criminality issues (Katyal, 2001;

Cronin, 2001). In some cases, local members of the judiciary and civil officers with power to administer and enforce law may lack knowledge about cybercrime (GAO Reports June 22, 2007). Since most countries lack comprehensive cybercrime laws, it complicates the extradition of a suspected cyber-criminal to the United States (Gabrys, 2002). Moreover, without federal assistance, state and local officials may not be able to extradite persons from other nations (GAO Reports June 22, 2007). The above discussion indicates that regulatory arbitrage is likely to be higher in cybercrimes compared to most conventional crimes.

That being said, it is also the case that some encouraging signs have emerged in recent years to suggest an improving international collaborations on cybercrimes. For instance, the US FBI also announced in May 2009 that it would permanently base a computer crime expert in Estonia to help fight international threats against computer systems (Associated Press Worldstream, May 11, 2009).

Interpol played a critical role to catch a member of Cyber Lords in Japan. The US federal agents have partnered closely with their counterparts in countries such as Egypt, Romania, Turkey, and Germany. As of 2003, 60 Romanian hackers were arrested in joint operations involving the FBI, Secret Service, Scotland Yard, the US Postal Inspection Service, and a number of European police agencies (Romania Gateway, 2003). As of 2008, Romania's national police and the FBI arrested 90 Romanians engaged in cybercrime activities. Likewise, Russian agents were trained in the United States (Swartz, 2008). 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). In October 2009, law-enforcement agencies in the United States and Egypt charged 100 people engaged in a phishing operation, who stole over $1.5 million from Bank of America and Well Fargo customers (Goodin, 2009). Fifty-three were from the US states of California, Nevada, and North Carolina and 47 were from Egypt.

In most cybercrimes, offenders and victims live in different jurisdiction. Industrialized countries have resources and a high-victimization level forced them to develop anti-cybercrime institutions. As noted above, many developing countries lack these conditions. Inter-jurisdictional collaborations and cooperation among law-enforcement agencies are "notoriously slow and bureaucratic" (Walden, 2005).

We would further argue that the issue here is not one of the existence of cybercrime laws,[1] but of enforcement mechanisms. Indeed, many developing economies have enacted cybercrime laws. In 2006, the United Arab Emirates (UAE) became the first country in North Africa and the Middle East to pass legislation on cybercrime and cyber-terrorism (Cybercrime Law, 2009; Ryan, 2009). Saudi Arabia followed the UAE in the same year (itp.net, 2006). Many of the 46 nations that had signed the CoE Treaty as of August 2009 are developing economies (COE, 2009). Diffusion patterns of cybercrime-related laws in some non-CoE developing economies are presented in Table 7.3.

A Saudi official noted that while cybercrime laws in Saudi Arabia offers basic legal measures, they lack details of technical and procedural measures required to prosecute cyber-criminals (Pinaroc, 2009). ITU secretary general Hamadoun Touré

Table 7.3 Diffusion of cybercrime-related laws in non-COE developing economies

Country	Status of cybercrime legislation
Botswana	October 2007: The cybercrime and computer-related Crimes Bill published in Government Gazette[a] December 2007: Parliament adopted the Bill with amendments by Minister of Communications
Gambia	October 2008: A draft Information and Communications Bill 2008, including computer misuse and cybercrime issues introduced[b]
India	October 2000: Information Technology Act, 2000 came into force December 2008: Information Technology (Amendment) Bill 2008 passed by Indian Parliament[c]. February 2009: The IT (Amendment) Act 2008 received the assent of the President[c] October 2009: The IT (Amendment) Act 2008 came into force[d]
Indonesia	July 2005: The Electronic Transaction and Information Law submitted to the House[b] March 2008: The parliament approved the proposed draft Cyber Law[e]
Kenya	January 2009: The Kenya Communications (Amendment) Act passed by the Parliament and signed into law by the President[b]
Macao	June 2009: A cybercrime bill drafted by the Macao Special Administrative Region (SAR) government was passed by local Legislative Assembly[f]
Malaysia	1997: Computer Crime Act 1997 introduced[g].
Nigeria	2005: Computer security and critical information infrastructure protection bill 2005 (Sb254) introduced to the National Assembly[b]
Pakistan	January 2007: A cybercrime Bill titled the Prevention of Electronic Crimes Bill 2006 has been adopted by the Federal Cabinet.[b] The President issued a decree, which made cybercrime "punishable with death or imprisonment with heavy fines"
Saudi Arabia	*October 2006: The Shariah Council* passed the first legislation to address electronic crime[h]
South Africa	July 2002: The Electronic Communications and Transactions Act, passed in 2002, has so far failed to prevent the proliferation (Assented)[i]
Thailand	July 2007: The Computer Crime Act took effect
The Philippines	2005: The government submitted an anti-cybercrime draft bill (not passed by Congress until April 2008)[j]
Uganda	June 2008: Draft electronic laws approved by Cabinet[k]
United Arab Emirates	February 2006: Cyber-Crime Law No. 2 issued by the President[b]
Zambia	August 2004: Parliament passed The Computer Misuse and Crimes law[l]

[a]Motlogelwa (2007).
[b]Cybercrime Law (2009).
[c]alertindian.com (2009).
[d]Business Standard (2009).
[e]Handayani (2008).
[f]chinadaily.com.cn (2009).
[g]bernama.com (2007).
[h]itp.net (2006).
[i]Government Gazette (2002).
[j]Yeo (2008).
[k]Kisambira (2008).
[l]ITU (2008).
[m]Khan (2008).

noted, "It [a global coalition] needs an organisational structure with a well-equipped cyber response team, all trained to similar levels across the globe – otherwise cybercriminals will locate themselves at the weakest point" (Bailey, 2009). Jurisdictional arbitrage is thus more than a matter of the existence of cybercrime laws and their enforcement.

7.3.1.2 Normative Institutions: Social Justifiability of Cybercrimes

Cybercrimes are more justifiable in some societies compared to others. Similarly, many Indonesian hackers feel that cyber-fraud is wrong, but acceptable if the victim is from a developed country (see Box 7.2). The above cybercrime behaviors can be reasonably explained by focusing on "higher" level existing institutions and exogenous parameters (Snidal, 1994, 1996). The hackers' views and perceptions, for instance, are similar to those of some historians and economists who argue that in the current global trading order, rich countries have exploited the developing world (Bemis, 1957; Bales, 1999; Buzzanco, 1999). Buzzanco (1999), for instance, argues that during the Cold War, the United States established a "hegemonic" trading order and imposed a global market that took advantage of the rest of the world to increase American companies' profit. This notion seems to be implicit in the arguments of many developing world-based hackers and computer criminals that are targeting industrialized world-based businesses and consumers.

7.3.1.3 Cognitive Institutions: Ideology

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." Ideology is an important component of cognitive institutions that energizes the behavior of many computer hackers. A number of cyberattacks are linked with fights for ideology. Ideological hackers attack websites to further political purposes. Such hackings can be mapped with obligation/community-based intrinsic motivations (Deci & Ryan, 1985; Lindenberg, 2001).

Prior researchers have also noted the important role of the community-based clan control to fight crimes (Chua, Huang, Wareham, & Robey, 2007). Community-based and formal control mechanisms, however, complement, contradict, oppose, or support each other (Chua et al., 2007). While some ideological hackers express nationalistic longings (see next section and Box 7.3) by acting up in line with the government (de Kloet, 2002), others act against their own nation or state. Prior researchers have recognized that communities may sanction breaking laws that are perceived as discriminatory or oppressive (Kane, 2002).For instance, in the mid-2001, Cyberjihad, a group of hackers in Indonesia attacked the website 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 7.3 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 public participation (Weber, Loumakis, & Bergman, 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

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's 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 of source, he argues that some nationalism are product of grass-root voluntarism (as US 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, 1987; 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[8]] provide the conceptual warp and woof of China's 'racial' nationalism."

Chinese Hackers' Patriotic and Nationalistic Longings

Chinese hackers have expressed 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 United States–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 US embassy in China and replaced the home page with racist and anti-government slogans (Denning, 2000). Following the collision of a US 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 United States, Brazil, and Europe attacked Chinese websites. According to a NewMax.com Wires article, Chinese hackers attacked about 1,100 US sites while American hackers broke into 1,600 Chinese sites (NewMax.com Wires, 2001). Similarly, after the collision of a Chinese fighter jet with a US surveillance plane in April 2001, Chinese hacking group attacked hundreds of US websites 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 hackers left the following message, "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. Patriotism and nationalism have thus provided cognitive legitimacy of these hackers' activities.

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 United States, Britain, Australia, and other coalition partners as well as domestic networks of Russia, Turkey, Indonesia, Pakistan, Saudi Arabia, Morocco, and Kuwait.

Another example of ideological hacking is the *Milworm* group's attack the website of India's Bhabha Atomic Research Center (BARC) (Chap. 3). 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

Nationalism and patriotism[2,3] can be considered as conceptual subsets of ideology. These are universally accepted as vital elements of state strength (Alagappa, 1995, 26–27). 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, cyberattacks 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.

Interestingly, Israel–Palestine tensions have a powerful virtual dimension. From October 2000 to January 2001, escalation in Israel–Palestine tensions resulted in attacks on 250 websites, which included networks of foreign companies and groups outside the Middle East (Adams, 2001).

Nationalism and patriotism were dominant codes of appeal in the United States–China cyber-wars of April–May 2001 (Box 7.3). Quoting a security engineer from Guangdong Province of China, *Netease* reported the daily number of attacks increased by over 20 times the average during April–May 2001. Analyzing the United States–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 unrealistic understanding of how the Internet functions as a medium for human interaction."

7.3.1.4 Stock of Cybercrime 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.

As discussed in Chap. 2, crime rates are tightly linked to the lack of economic opportunities. Also addressed in much empirical study are linkages of crime and other deviant behaviors with people living in poverty (Oxoby, 2004). 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). A financial crash in 1998 left many computer programmers unemployed, worsening the situation. 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). On the other hand, the primary reason behind India's low-cybercrime profile is the existence of a well-developed legitimate IT industry in the country (Greenberg, 2007).

A large number of extortion-related cyberattacks originate from Eastern Europe and Russia (see Box 7.1). Hackers in these economies 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 (newpaper.asia1.com.sg, 2004). Russian hackers have a deep understanding of networks and know how to "get in and out without a trace" (Walker, 2004). Consider the US National Security Agency-backed "hacking" competition of June 2009. Four thousand two hundred programmers from all over the world participated in algorithm coding and other contests. Of the finalists in the competitions, 20 were from China, 10 were from Russia, and only 2 were from the US (Cetron & Davies, 2009).

7.3.2 Profile of Target Organization

7.3.2.1 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). One can draw a parallel—or an analogy—to what is seen in cyberattacks. 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 US hackers attacked each other's websites. Each camp selected websites that had symbolic values. In the United States, 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). Speaking of challenges facing the US Defense Department, Robert Lentz, deputy assistant Defense secretary

for information and identity assurance, noted that the Pentagon "is the number-one target" for cyberattacks (Campbell, 2008).

7.3.2.2 Digitization of Value and Target Attractiveness

As to the target attractiveness (Chap. 2), it is worth noting that crimes target sources of value, and for this reason, digitization of value is tightly linked with digitization of crime. Regarding the devastating impact of the 2007 cyberattacks against Estonia, it is important to note that, by 2007, Estonia had implemented various high-profile, e-government projects. For instance, 90% of banking services, and parliamentary elections, were conducted online (BBC News, 2007).

Cybercrimes' impacts are clearly skewed towards rich economies, large companies, and high-income people. As noted earlier, the United States is the world's No. 1 cybercrime target. Analysts suggest that the Gulf region's oil-fueled prosperity has made the region attractive cybercrime target. In the Gulf Cooperation Councils (GCC) economies, for instance, in the first 9 months of 2009, there were over 769,000 instances of "compromised systems breakdown" in Saudi Arabia, 248,000 in the UAE, 95,000 in Kuwait, 60,000 in Bahrain, and 37,000 in Oman (Gulf Daily News, 2009).

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. A survey conducted among Australian firms indicated that average looses of a cybercrime were A $360 small businesses, A $2,757 medium businesses, and A $17,578 for large businesses (Andrews, 2009).

A study indicated that high-income earners (more than £50,000 a year) in the United Kingdom are 3–5 times more likely to become victims of identity fraud than the average UK resident (Heera, 2008; cf. Rush, Chris Erika, & Puay, 2009). Likewise, in Bangladesh, businesspersons, contractors, and wealthy people have been targets of extortion activities that use cellphones with unregistered subscriber identity module (SIM) cards (The New Nation, 2009).

Businesses with a high dependence on digital technologies—including online casinos, banks, and e-commerce hubs—are more likely to be the target 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).

7.3.2.3 Weakness of Defense Mechanisms

Weakness of defense mechanism co-varies positively with the likelihood of an attack (Glaeser & Sacerdote, 1999). In this regard, it is important to note that computer systems contain many flaws. Such flaws can be attributed to factors such as complexity, rapid change in the software industry, and a lack of penalties for companies that develop flawed software (Mann, 2002). Hackers in most cases take advantage

of these flaws. It is important to note that hundreds of millions of computers that are connected to the Internet have security holes. While many of them are easily fixable, many are undiscovered. Due to weak defenses of most computer networks, it is also difficult to track origins of cyberattacks (Kong and Swartz, 2000).

7.4 Concluding Comments

This chapter has contributed to the conceptual and empirical understanding of global cyber-wars and crimes. The analyses of this chapter 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.

Nations across the world differ widely on key elements represented by Fig. 7.1 and hence on domestic/foreign composition of sources and targets of cyberattacks as well as attackers' motivations. For instance, societies that have weak or no cybercrime laws and where socio-cultural practices provide some degree of legitimacy to such crimes are likely to provide fertile ground for these crimes. To illustrate from the US perspective, in Table 7.4, we have classified targeted cyberattacks impacting the US by national border in terms of target and source.

For industrialized economies, the battle against cybercrime is about more than just developing capacity on the home front. Important technological issues crossing national borders can be better dealt with at policy levels (Skolnikoff, 1989). International collaborations are, however, lacking with law-enforcement agencies in some of the top cybercrime sources. For instance, it is reported that government officials in Nigeria claimed that they were ignorant of Internet crimes originated from Nigeria and some labeled it as Western propaganda (Lawal, 2006). In general, a lack of legal infrastructures and enforcement mechanisms in developing countries has increased the jurisdictional arbitrage (Table 7.5).

When law-enforcement agencies in developing economies are genuinely engaged in fighting cybercrime activities targeting foreign countries, the likelihood of them controlling such activities is much greater than when a foreign government simply imposes them to do so. From the US standpoint, it is worth noting that the United

Table 7.4 Classification of targeted cyberattacks by national border: an illustration from the US 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] • US 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 US companies • Foreign cyber scammers targeting US companies/Internet users • Foreign organized criminal groups (e.g., Russian online extortionists) targeting US companies • Foreign government agencies (e.g., the government of Burma sending virus-attached e-mails to its critics residing in the US) • Foreign patriotic/nationalistic hackers (e.g., Chinese attacking US 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 US diplomatic offices (e.g., The China-based Level Seven Crew's attack on the website of the US embassy in China)

States is facing an image problem in many countries that are among the top cybercrime sources (Tables 7.1 and 7.2): According to the 2009 Pew Global Attitudes Survey conducted by the Washington, DC-based Pew Research Center, only 14% Turkish, 16% Pakistanis, 27% of Egyptians, 38% Argentinanians, 44% of Russians, and 47% of Chinese have a favorable view of the United States (Pew Research Center, 2009). Likewise, a survey conducted by the BBC and the University of Maryland in April 2008 found that people in 23 countries viewed US influence in the world more negatively than that of North Korea (Debusmann, 2008).

One view is that, the US foreign policy would be drastically different in Obama's administration, which is likely to lead to a more positive image of the US worldwide (Debusmann, 2008). The opposite argument is that there really are no fundamental

Table 7.5 Measuring the cybersafety environment

Stage of cybersafety	Institutional indicators	Business-related indicators
Number of attacks per 1,000 Internet users	Existence of laws that require appropriate defense mechanisms (+)	Proportion of revenue spent in network security (+)
Proportion of cyberattacks 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 (+)	Willingness of cybercrime victims to report crimes (+)
	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 cyberattacks (–)	

Note: +: positive contribution to cybersafety; –: negative contribution to cybersafety.

differences in the foreign policy approaches of the new and the old government. Arguing that Obama's approach is likely to be "surprisingly similar" to George W. Bush, Posner (2009) notes: "The United States—under the leadership of both the Republican and Democratic parties—has taken a fairly consistent approach to international law over the decades, one that involves building legal regimes that serve US interests and tearing down those that do not." If this view is substantially correct, it seems clear that the cybercrime fighting efforts of the United States are likely to face serious difficulties in some of the top cybercrime sources.

Notes

1. For instance, the law enacted in Romania in 2003 punishes convicts with up to 15 years in prison (Romania Gateway, 2003).
2. 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 ethnonational superiority" (Pei, 2003). Brown (1999) considers patriotism as identification with territory whereas nationalism as identification with the group. We use the terms nationalism and patriotism interchangeably.
3. 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, nationalism on consumer ethnocentrism in Turkey and the Czech Republic, Balabanis, Diamantopoulos, Mueller, and Melewar (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.

4. 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). Accessed 27 October 2004.
5. Online casinos rely on Worldpay to process customer's transactions and pay off gamblers (Walker, 2004).
6. "Russia's Hackers: Notorious or Desperate?" CNN.com. November 20, 2000. http://www.cnn.com/2000/TECH/computing/11/20/russia.hackers.ap/index.html (Accessed 27 October 2004).
7. A carder is a person who uses stolen credit card information to buy items online.
8. Archaeology is the study of ancient societies and cultures. Paleoanthropology is the study of the human fossil record.

References

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

Alagappa, M. (1995). *Political legitimacy in Southeast Asia.* Stanford, CA: Stanford University Press.

alertindian.com. (2009). Cyber crime laws in India. http://www.alertindian.com/node/5. Accessed 27 October 2009.

Andrews, L. (2009, June 9). Online scams go unreported and unpunished. *Cybercriminals Beating the Law Canberra Times* (Australia) SECTION: A; 5.

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

Associated Press Worldstream. (2009). FBI to station cybercrime expert in Estonia.

Bailey, D. (2009, September 30). ITU pledges to fight global cybercrime, *Computing*. http://www.computing.co.uk/computing/analysis/2250377/q-international. Accessed 27 October 2009.

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.

Bales, K. (1999). *Disposable people: New slavery in the global economy.* Berkeley, CA: University of California Press.

Barme, G. (1999). *In the red: On contemporary Chinese culture*. New York: Columbia University Press.

BBC News. (2007) Estonia hit by 'Moscow cyber war'. http://news.bbc.eo.uk/2/hi/europe/6665145.stm. Accessed 27 October 2009.

Bemis, S. F. (1957). *The diplomacy of the American revolution*. Bloomington, IN: Indiana University Press.

bernama.com. (2007). Malaysia Should Focus More On Enforcing Cyber Law, Says Microsoft, December 12, 2007. http://www.bernama.com/kpdnhep/news.php?id=302117&lang=en. Accessed 27 October 2009.

Blau, J. (2004, May 28). Viruses: From Russia, with love? *IDG News Service*. http://www.pcworld.com/news/article/0,aid,116304,00.asp. Accessed 27 October 2006.

Bridis, T. (2001). E-Espionage rekindles cold-war tensions – US Tries to identify hackers; millions of documents are stolen. *Wall Street Journal*, A.18.

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

Business Standard. (2009). Amended IT Act to prevent cyber crime comes into effect, October 27, 2009. http://www.business-standard.com/india/news/amended-it-act-to-prevent-cyber-crime-comes-into-effect/21/19/76884/on. Accessed 11 April 2010.

Buzzanco, R. (1999). What happened to the new left? Toward a radical reading of American foreign relations. *Diplomatic History*, 575–608.

Campbell, D. (2008, April 1). Lentz: Content-centricity key to DOD communications. *Government Computer News*. http://gcn.com/articles/2008/04/01/lentz-contentcentricity-key-to-dod-communications.aspx.

Cetron, M. J., & Davies, O. (2009). Ten Critical Trends for Cybersecurity. *Futurist, 43*(5), 40–49.

chinadaily.com.cn. (2009). Macao passes cyber-crime bill, 2009-06-25. http://www.chinadaily.com.cn/china/2009-06/25/content_8324247.htm. Accessed 27 October 2009.

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

Chua, C., Huang, E., Wareham, J, & Robey, D. (2007). The role of online trading communities in managing internet auction fraud. *MIS Quarterly, 31*(4), 759–781.

CNN.Com. (2000, January 10). Rebuffed Internet extortionist posts stolen credit card data. http://cnn.com/2000/TECH/computing/01/10/credit.card.crack.2/index.html. Accessed 27 October 2005.

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

COE. (2009). Convention on Cybercrime: CETS No.:185. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG. Accessed 27 October 2009.

Comité Européen Des Assurances. (2004, February). 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*. http://www.cea.assur.org/cea/v1.1/actu/pdf/uk/annexe180.pdf. Accessed 27 October 2006.

Cronin, B. (2001). Information warfare: Peering inside Pandora's postmodern box. *Library Review, 50*(6), 279–295.

Cybercrime Law. (2009). News. http://www.cybercrimelaw.net.

Darmosumarto, S. (2003, December 8). Battle on Internet credit card fraud still long. *The Jakarta Post*. http://www.crime-research.org/news/2003/12/Mess0802.html. Accessed 27 October 2006.

Datamonitor. (2009, July). eBay, Inc. *SWOT Analysis*, 1–9.

de Kloet, J. (2002). Digitisation and its Asian discontents: The Internet, politics and hacking in china and Indonesia. *First Monday*, 7(9). http://firstmonday.org/issues/issue7_9/kloet/index.html. Accessed 1 October 2005.

Debusmann, B. (2008, November 13). Obama and a makeover for the 'ugly American'. http://www.nytimes.com/2008/11/13/world/americas/13iht-letter.1.17790862.html. Accessed 27 October 2009.

Deci, E. L, & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behavior*. New York, NY: Plenum Press.

Deloitte Touche Tohmatsu. (2002). *Australian computer crime and security survey*. http://www.4law.co.il/346.pdf. Accessed 27 October 2005.

Dempsey, P. J. (2008). Unprepared to fight worldwide cyber crime. http://www.internetevolution.com/author.asp?section_id=593&doc_id=147027&piddl_msgid=154774#msg_154774. Accessed 27 October 2009.

Denning, D. E. (2000). Hacktivism: An emerging threat to diplomacy. *American Foreign Service Association*. www.afsa.org/fsj/sept00/Denning.cfm. Accessed 27 October 2004.

Duk-kun, B. (2003, November 19). Largest Internet hacking ring uncovered. *The Korea Times*.

Etges, R., & Sutcliffe, E. (2008). An overview of transnational organized cyber crime. *Information Security Journal: A Global Perspective, 17*(2), 87–94.

Foreign Policy. (2005, March/April). Caught in the net: Australian teens, 92.

Forensic Accounting Review and Computer Security Digest. (2001). FBI warns of Russian hackers stealing US credit-card data. *17*(8), 2.

Gabrys, E. (2002). The international dimensions of cyber-crime, Part 1. *Information Systems Security, 11*(4), 21–32.

GAO Reports. (2007). *Public and private entities face challenges in addressing cyber threats*. RPT-Number: GAO-07-705.

Giannangeli, M. (2008, June 8). Are we ready for Russian Mafia's crime revolution? *Sunday Express*, Scottish Edition, 4.

Glaeser, E. L., & Sacerdote, B. (1999). Why is there more crime in cities? *The Journal of Political Economy, 107*(6), Part 2, S225–S258.

Godoy, J. (2000). Computers and International Criminal Law: High Tech Crimes and Criminals. *New England International and Comparative Law Annual*, 6. http://www.nesl.edu/intljournal/vol6indx.cfm. Accessed 27 October 2005.

Gomes, L., & Bridis, T. (2001, March 9). FBI warns of Russian hackers stealing credit-card data from US computers. *Wall Street Journal*, A.4.

Goodin, D. (2009, October 8). Feds net 100 phishers in biggest cybercrime case ever. http://www.theregister.co.uk/2009/10/08/100_phishers_netted. Accessed 27 October 2009.

Government Gazette. (2002, August 2). Act No. 25, 2002 Electronic Communications and Transactions Act, 2002, Government Gazette. http://web.uct.ac.za/depts/shiplaw/fulltext/electcomsact.pdf. Accessed 27 October 2006.

Greenberg, A. (2007). The top countries for cybercrime. *Forbes.com*. http://www.forbes.com/2007/07/13/cybercrime-world-regions-tech-cx_ag_0716cybercrime.html. Accessed 27 October 2008.

Grow, B., & Bush, J. (2005, May 30). Hacker hunters. *Business Week*, 2005.

Gulf Daily News. (2009, October 23). Cyber crime alert. *gulf-daily-news.com.* http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=262426. Accessed 23 October 2009.

Hahn, R.W., & Layne-Farrar, A. (2006). The law and economics of software security. *Harvard Journal of Law and Public Policy, 30*(1), 283–353.

Handayani, R. (2008, June 13). Indonesia: Introducing the first Indonesian Cyber law. http://asia.legalbusinessonline.com/regional-updates/25196/details.aspx. Accessed 27 October 2009.

Handelman, S. (1999, September 20). Russia's rule by racketeers. *Wall Street Journal*, A.28.

Hansen, M. (1999). *Lessons in being Chinese: Minority education and ethnic identity in Southwest China*. Seattle: University of Washington Press.

Havely, J. (2000, February 16). Online's when states go to cyber-war. *BBC News*.

Heera, S. (2008). Directors of larger dealerships at significant risk of identity theft, warns Experian, New Release. *Experian.com*. http://press.experian.com/documents/showdoc.cfm. Accessed 27 October 2009.

Interpol. (2007). INTERPOL's six priority crime areas. http://www.interpol.int. Accessed 27 October 2008.

Ismail, I. (2008, February 18). Understanding cybercriminals. *New Straits Times* (Malaysia), 12.

itp.net. (2006, October 15). Saudi passes cybercrime laws. http://www.itp.net/487865. Accessed 27 October 2009.

ITU. (2008). ITU Regional Cybersecurity Forum 2008 Lusaka, Zambia, Meeting Report: ITU Regional Cybersecurity Forum for Eastern and Southern Africa, Lusaka, Zambia, 25–28 August 2008, 29 August 2008. http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/lusaka-cybersecurity-forum-report-aug-08.pdf. Accessed 27 October 2009.

Jewkes, Y., & Andrews, C. (2005). Policing the filth: The problems of investigating online child pornography in England and Wales. *Policing & Society, 15*(1), 42–62.

Kane, R. J. (2002). The social ecology of police misconduct. *Criminology, 40*(4), 867–896.

Katyal, N. K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review, 149*(4), 1003–1114.

Khan, M. I. (2008). Pakistan unveils cybercrime laws, 7 November 2008. http://news.bbc.co.uk/2/hi/7714714.stm. Accessed 27 October 2009.

Kirk, J. (2009, March 11). Countries move forward on cybercrime treaty. *PC World*. http://www.pcworld.com/article/161067/countries_move_forward_on_cybercrime_treaty.html. Accessed 27 October 2009.

Kisambira, E. (2008, October, 6). Uganda cyber laws going to parliament. http://www.networkworld.com/news/2008/100608-uganda-cyber-laws-going-to.html. Accessed 27 October 2009.

Kluver, R. (2001). New media and the end of nationalism: China and the US in a war of words. *Mots Pluriels*. www.arts.uwa.edu.au/MotsPluriels/MP1801ak.html. Accessed 27 October 2009.

Kong, D., & Swartz, J. (2000, September 27). Experts see rash of hack attacks coming recent costly hits show 'more brazen' criminals preying on companies. *USA Today*, 01.B.

Krebs, B. (2007, October 13). Taking on the Russian Business Network. http://blog.washingtonpost.com/securityfix/2007/10/taking_on_the_russian_business.html. Accessed 27 October 2009.

Kshetri, N. (2005, May/June). Hacking the odds. *Foreign Policy*, 93.

Lawal, L. (2006, May 22). Online scams create "Yahoo! millionaires": In Lagos, where scamming is an art, the quickest way to wealth for the cyber-generation runs through a computer screen. *Fortune*. http://money.cnn.com/magazines/fortune/fortune_archive/2006/05/29/8378124/. Accessed 27 October 2009.

Lemos, R. (2001, May 1). FBI "hack" raises global security concerns. *CNet News*. http://news.com.com/2100-1001-950719.html

Levi, M. (2002). The organization of serious crimes. *The Oxford Handbook of Criminology* (pp. 878–913). Oxford: Oxford University Press.

Leyden, J. (2009, October 22). FBI and SOCA plot cybercrime smackdown. *The Register.* http://www.theregister.co.uk/2009/10/22/soca_fbi_cybercrime_strategy/ Accessed 27 October 2009.

Lieberman, D. (2003). Feds enlist hacker to foil piracy rings; Plea agreement includes help in satellite TV cases. *USA Today*, January 10, B.01.

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.

Lindenmayer, I. (2006). *Online American Banker, 171*(18), 6.

Lorek, L. (2001). Russian Mafia net threat. *Interactive Week*, 11.

Mann, C. C. (2002, July–August). Why software is so bad. *Technical Review*, 33. http://www.technologyreview.com/InfoTech/wtr12887,300,p1.html. Accessed 27 October 2005.

Motlogelwa, T. (2007, October 5). Cyber crime law gets teeth. http://www.mmegi.bw/index.php?sid=1&aid=30&dir=2007/October/Friday5. Accessed 27 October 2009.

Muncaster, P. (2006, December 11). Organised crime gangs lure IT graduates. *IT Week*, http://www.businessgreen.com/itweek/news/2170640/organised-crime-gangs-lure. Accessed 18 March 2010.

Naím, M. (2005). *Illicit: How smugglers, traffickers, and copycats are hijacking the global economy.* New York: Doubleday.

NewMax.com Wires. (2001, May 21). Chinese hackers may be rallying forces. http://archive.newsmax.com/archives/articles/2001/5/22/84452.shtml. Accessed 27 October 2005.

newpaper.asia1.com.sg. (2004, August 3). Hackers – The new breed of gangsters. http://newpaper.asia1.com.sg/top/story/0,4136,69503-1-1098892740,00.html. Accessed 27 October 2005.

ohchr.org (2007, April) Report by the Kharkiv Human Rights Protection Group about Ukraine's compliance with the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. http://www2.ohchr.org/english/bodies/cat/docs/ngos/khrpg.doc Accessed 27 October 2009.

Oksenberg, M. (1987). China's confident nationalism. *Foreign Affairs, 65*(3), 501–523.

Ong, A. (1997). Chinese modernities: Narratives of nation and of capitalism. In A. Ong & D. Nonini (Eds.), *Underground empires: The cultural politics of modern Chinese transformation*. New York: Routledge.

Onlinecasinonews.com. (2004, February 3). Mob's extortion attempt on Internet bookies. http://www.onlinecasinonews.com/ocnv2_1/article/article.asp?id=4748. Accessed 27 October 2005.

Oxoby, R. J. (2004). Cognitive dissonance, status and growth of the underclass. *Economic Journal, 114*(498), 727–749.

Peer, B. (2001, July 10). Lashkar web site hacked. http://www.rediff.com/news/2001/jul/10hack1.htm. Accessed 27 October 2005.

Pei, M. (2003). The paradoxes of American nationalism. *Foreign Policy, 136*, 30–37.

Pew Research Center. (2009). Opinion of the United States. http://pewglobal.org/database/?indicator=1&mode=chart. Accessed 27 October 2009.
Pinaroc, J. D. (2009, October 14). Saudi faces tough time with cybercrimes. *ZDNet Asia*. http://www.zdnetasia.com/news/security/0,39044215,62058637,00.htm. Accessed 27 October 2009.
Porter, M. E. (2001). Strategy and the Internet. *Harvard Business Review, 79*(3), 63–78.
Posner, E. (2009). Think again: International law: Governments respect international law only when it suits their national interests. Don't expect that to change any time soon.
Regan, K. (2006) FBI: Cybercrime causes financial pain for many businesses. *TechNewsWorld*. http://www.technewsworld.com/story/48417.html. Accessed 27 October 2008.
Richmond, R. (2003, January 27). Selling strategies – Scammed! Web merchants use new tools to keep buyers from ripping them off. *Wall Street Journal*, R.6.
Riptech. (2002, July). *Riptech internet security threat report* (Vol. II). http://www.4law.co.il/276.pdf. Accessed 27 October 2005.
Rogers, E. M. (1983). *The diffusion of innovations* (3rd ed.). New York: Free Press.
Romania Gateway. (2003, October 24). Romania emerges as nexus of cybercrime. http://rogateway.ro/node/185929/comnews/item?item_id=223937. Accessed 27 October 2006.
Rosenau, J. N. (1995). Security in a turbulent world. *Current History, 94*(592), 193–200.
Rush, H., Chris, S., Erika, K. M., & Puay, T. (2009). Crime online: Cybercrime and illegal innovation. Research report: July 2009, CENTRIM, University of Brighton. http://eprints.brighton.ac.uk/5800/01/Crime_Online.pdf. Accessed 27 October 2009.
Ryan, Y. (2009). Algerian bloggers feel threatened by proposed law. http://www.nytimes.com/2009/09/21/technology/21iht-censor.html, September 21, 2009. Accessed 27 October 2009.
Salmon, P. (1995). Nations competing against themselves: An interpretation of European integration. In A. Breton, G. Galeotti, P. Salmon, & R. Wintrobe (Eds.), *Nationalism and rationality.* Cambridge: Cambridge University Press.
Sautman, B. (2001). Peking man and the politics of paleoanthropological nationalism in China. *The Journal of Asian Studies, 60*(1), 95–124.
Serio, J. D., & Gorkin, A. (2003). Changing lenses: Striving for sharper focus on the nature of the 'Russian Mafia' and its impact on the computer realm. *International Review of Law, Computers and Technology, 17*(2), 191–202.
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, February 6). Taking a swipe at cyber card fraud. *CNN.com*. http://www.cnn.com/2003/WORLD/asiapcf/southeast/02/06/indonesia.fraud. Accessed 27 October 2006.
Simpson, P. (1993). *Language, ideology and point of view.* London/New York: Routledge.
Skolnikoff, E. B. (1989). Technology and the world tomorrow. *Current History, 88*(534), 5–13.
Smith, C. S. (2001, May 13). The first world hacker war. *New York Times*, 4.2.
Snidal, D. (1994). The politics of scope: Endogenous actors, heterogeneity and institutions. *Journal of Theoretical Politics, 6*(4), 449–472.
Snidal, D. (1996). Political economy and international institutions. *International Review of Law and Economics, 16*(1), 121–137.
sophos.com. (2004, July 23). Police crack suspected online extortion ring. *Sophos reports*. http://www.sophos.com/virusinfo/articles/extortion.html.
sophos.com. (2008, July 23). Police crack suspected online extortion ring. *Sophos reports*. http://www.sophos.com/virusinfo/articles/extortion.html. Accessed 27 October 2009.
Steffensmeier, D., & Ulmer, J. T. (2006). Black and white control of numbers gambling: A cultural assets-social capital view. *American Sociological Review, 71*(1), 123–157.
Sullivan, B. (2004, April 1). Foreign fraud hits US e-commerce firms hard. *MSNBC*. http://www.msnbc.msn.com/id/4648378. Accessed 27 October 2005.
Sutherland, B. (2008). The rise of black market data; Criminals who steal personal data often don't exploit it. Instead, they put it up for sale on one of the many vibrant online markets. *Newsweek, 152*(24) (International ed.).
Swartz, J. (2004, October 21). Crooks slither into Net's shady nooks and crannies crime explodes as legions of strong-arm thugs, sneaky thieves log on. *USA Today.* www.usatoday.com/printedition/money/20041021/cybercrimecover.art.htm. Accessed 2 October 2005.

Swartz, J. (2008, November 17). Hackers, phishers can't get away with it like they used to, *USA Today*, http://www.usatoday.com/money/industries/technology/2008-11-16-hackers-phisher-crime-fbi_N.htm. Accessed 18 March 2010.

Symantec. (2004). *Symantec internet security threat report* (Vol. VI). http://www.4law.co.il/L138.pdf. Accessed 2 October 2005.

Tedjasukmana, J. (2002, September 23). The no-payment plan: Thousands of young Indonesians commit cyberfraud for fun and profit. http://www.time.com/time/globalbusiness/article/0,9171,1101020923-351237,00.html. Accessed 27 October 2005.

The Economist Intelligence Unit Limited. (2008). Country Commerce, Indonesia, 77–81. www.eiu.com. Accessed 27 October 2009.

The Economist. (2003, November 29). Special report: Fighting the worms of mass destruction – Internet security, 101.

The Happy Hacker. (2001).The US/China cyberwar of April/May 2001. http://www.happyhacker.org/news/china.shtml. Accessed 27 October 2005.

The New Nation. (2009, October 5). Cell phone crime rise: Extortions go on unabated, Internet Edition. http://nation.ittefaq.com/issues/2009/10/05/news0827.htm. Accessed 27 October 2009.

Varese, F. (2002). *The Russian Mafia: Private protection in a new market economy*. New York: Oxford University Press.

Walden, I. (2005). Crime and security in cyberspace. *Cambridge Review of International Affairs, 18*(1), 51–68.

Walker, C. (2004, June). Russian Mafia Extorts Gambling Websites. http://www.americanmafia.com/cgi/clickcount.pl?url=www.americanmafia.com/Feature_Articles_270.html. Accessed 27 October 2005.

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, August 13). Organized Crime and Cybercrime: Synergies, Trends, and Responses. Office of International Information Programs, US Department of State. http://usinfo.state.gov. Accessed 27 October 2005.

Winterford, B. (2009, October 12). Banks report 70 percent of phishing attacks hosted offshore. *IT News*. http://www.itnews.com.au/News/158011,banks-report-70-percent-of-phishing-attacks-hosted-offshore.aspx. Accessed 27 October 2009.

Yeo, V. (2008, April 15). Asia hindered by lack of cybercrime laws. http://www.businessweek.com/globalbiz/content/apr2008/gb20080415_220378.htm?chan=top+news_top+news+index_global+business. Accessed 27 October 2009.