Chapter 3
An Institutional Perspective on Cybercrimes

"The draft treaty is contrary to well-established norms for the protection of the individual" (The Global Internet Liberty Campaign's comment on Council of Europe's Treaty on Cybercrime, BBC News online December 18, 2000).

"Why are Brazil's hackers so strong and resourceful? Because they have little to fear legally" (Smith, 2003, quoting a Brazilian Internet security expert).

Abstract There are persuasive arguments for thinking that institutional processes have enormous power to explain cyberattacks. This chapter examines how macro- and micro-level institutions provide regulative, normative, and cognitive legitimacy to hackers', organizations', and governments' actions that facilitate or hinder cyberattacks. More specifically, we analyze institutions at supra-national, national, professional, industry, organizational, informal network, and intra-organizational levels in terms of their impacts on cyberinfrastructure, network, and computer attacks.

3.1 Introduction

The nature of activities of cyber-criminals fits squarely with what Baumol (1990) calls destructive entrepreneurship. Baumol (1990) hypothesized that the distribution of productive, unproductive, and destructive entrepreneurs in a society is a function of the "relative payoffs" offered to these activities by the society's "rules of the game." Note that these rules are referred as institutions (North, 1990). An entrepreneur's acts in an economy depend on the rules of the game and the reward structure in the economy (Baumol, 1990, p. 894).

Prior researchers have recognized that economic activities and actors are embedded in formal and informal institutions (Granovetter, 1985; Parto, 2005). There are persuasive arguments for thinking that institutional processes have enormous power to explain the degree and patterns of cyberattacks. An institutional perspective helps us link cyberattacks with rules and laws as well as values, norms, and cognitive assessment of actors related to cyberattacks.

N. Kshetri, *The Global Cybercrime Industry*, DOI 10.1007/978-3-642-11522-6_3,

Social and policy-related factors and institutional logics powerfully moderate the effects of economic forces (Schneiberg, King, & Smith, 2008). It is apparent that cybercrimes differ from other crimes in terms of permissiveness of regulatory regimes (Mittelman & Johnston, 1999), regulatory arbitrage (Levi, 2002), and culture and ethical attitudes that influence external and internal stigma (Aguilar-Millan, Foltz, Jackson, & Oberg, 2008; Donaldson, 1996; Kwong, Yau, Lee, Sin, & Tse, 2003).

In this chapter, we draw upon literatures on institutional theory to develop a framework on the institution-cybercrime nexus. More to the point, we provide a framework for key institutional factors at different levels of analysis that influence cyberattacks.

3.2 Institutional Theory

We begin by considering a broad approach to institutions, which defines the concept in terms of an equilibrium of a game. Three factors that determine an equilibrium include "(i) technologically determined external constraints; (ii) humanly devised external constraints, and; (iii) constraints developed within the game through patterns of behavior and the creation of expectations" (Snidal, 1996, p. 128). This section mainly deals with the second factor, which corresponds to the "rules of the game" and includes "formal constraints (rules, laws, constitutions), informal constraints (norms of behavior, conventions, and self-imposed codes of conduct), and their enforcement characteristics" (North, 1996, p. 344).

Scott (1995) proposed three institutional pillars—regulative, normative, and cognitive—which relate to "legally sanctioned," "morally governed," and "recognizable, taken-for-granted" behaviors, respectively (Scott, Ruef, Mendel, & Caronna, 2000, p. 238). Formal constraints can be mapped with Scott's (2001) regulative pillar while informal constraints can be mapped with normative and cognitive pillars. To put things in context, formal and informal institutions influence the perceived threats of shame and embarrassment and that of legal sanctions for a criminal (Blackwell, 2000; Grasmick & Robert, 1990).

3.2.1 Regulative Institutions

Regulative institutions consist of "explicit regulative processes: rule setting, monitoring, and sanctioning activities" (Scott, 1995, p. 35). These institutions focus on the pragmatic legitimacy concerns in managing the demands of regulators and governments (Kelman, 1987). In the context of this chapter, regulative institutions consist of regulatory bodies (such as the US Department of Justice and the US Department of Homeland Security) and existing laws and rules (e.g., *the Patriot Act* and *the Gramm Leach Bliley (GLB) Act* in the United States) that influence individuals and organizations to behave in certain ways (Scott, 1995). Individuals and organizations adhere to the rules so that they would not suffer the penalty for noncompliance (Hoffman, 1999).

3.2.2 Normative Institutions

Normative components introduce "a prescriptive, evaluative, and obligatory dimension into social life"[1] (Scott, 1995, p. 37). This component focuses on the values and norms held by individuals, organizations, and government agencies that influence the ICT-national security nexus. 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). The basis of compliance in the case of normative institutions derives from social obligations, and non-adherence can result in societal and professional sanctions. Normative institutions also include trade associations, professional associations (e.g., the Honker Union of China, also known as the Red Hackers), or non-profit organizations (e.g., ACLU in the US) that can use social obligation requirements (e.g., ethical codes of conduct) to induce certain behavior.

3.2.3 Cognitive Institutions

Cognitive institutions are associated with culture (Jepperson, 1991). These components represent culturally supported habits that influence governments', firms', and hackers' behaviors. In most cases, they are based on subconsciously accepted rules and customs as well as some taken-for-granted cultural account of computer use (Berger & Luckmann, 1967). Scott (1995, p. 40) suggests that "cognitive elements constitute the nature of reality and the frames through which meaning is made."

Although carried by individuals, cognitive programs are social in nature (Berger & Luckmann, 1967). Compliance in the case of cognitive legitimacy concerns is due to habits. Political elites, organizational decision makers, and hackers may not even be aware that they are complying.

3.2.4 Interrelationships Among Institutional Pillars

It is quite possible that formal and informal institutions with respect to some issues may be incongruent for some groups (Webb, Tihanyi, Ireland, & Sirmon, 2009). That is, what some groups in a society may consider some activities legitimate, as specified by their norms, values, and beliefs, which are in fact illegal, that, they violate existing laws and regulations (Dowling & Pfeffer, 1975; Webb et al., 2009).

It is, however, worth keeping in mind that an institutional pillar both reflects and determines the nature of the other pillars (Hayek, 1979). In the "real world," thus it is difficult to isolate them. North (1994) argues that informal rules such as values and norms provide legitimacy to formal rules. Likewise, political scientist Robert Axelrod (1997, p. 61) comments on the relationship between regulative and normative institutions:

> Social norms and laws are often mutually supporting. This is true because social norms can become formalized into laws and because laws provide external validation of norms.

3.2.5 Exogenous and Endogenous Institutions

Another approach to analyze institutions is to focus on the exogenous and endogenous natures (Davis & North, 1971). According to this approach, the exogenous institutional environment consists of formal and informal macro-level rules such as the judicial system, cultural norms, and kinship patterns (Davis & North, 1971). The exogenous institutional environment is slow to change and defines the world in which firms and people interact. Some refer these as *fundamental institutions*, which "are taken for granted and are difficult to change through purposive design" (Bresser & Millonig, 2003).The endogenous institutional arrangement, on the other hand, consists of the formal and informal micro-level rules of exchange devised by specific parties to a specific exchange (Davis & North, 1971; Carson, Timothy, Grahame, & George, 1999) or to regulate specific societal problems (Bresser & Millonig, 2003). These are also known as s*econdary institutions*. They include laws, contracts, organizations, and organizational rules and procedures and are more amenable to conscious design (Bresser & Millonig, 2003).

3.2.6 Neoinstitutionalism

Neoinstitutionalism is characterized by both macro- and micro-level approaches, which complement each other (Scott, 1987). One way to differentiate these two approaches is whether the sources of institutionalization are external or internal to the organization. Macro-institutionalism considers the sources of institutionalization in the external environment of organizations and argues that organizations exhibit isomorphism with respect to external institutional pressures by adopting institutionally desirable structures and processes. Micro-institutionalism, on the other hand, assumes that these sources are internal to organizations (Bresser & Millonig, 2003). Scott (1995, p. 40) observes the existence of external and internal dimensions in institutions by stating that values and norms ". . . are both internalized and imposed by others." Inter-firm differences in behavior can be explained in terms of an "institutional filter," which determines the extent to which specific environmental demands are compatible with an organization's system of norms and values and should therefore be adopted (Bresser & Millonig, 2003). Theorists have provided evidence, which indicates that organizations may engage in non-isomorphic responses if they perceive that such responses are likely to minimize a potential loss of resources (George, Chattopadhyay, Sitkin, & Barden, 2006).

Many micro-level rules that govern cyber-criminals' and victims' decisions and have extremely large macro-level consequences are embedded in the social and cultural institutions. Macro-level heterogeneity can thus arguably be attributed to "homophilic microlevel rules" (Macy & Willer, 2002, p. 13). Deinhart (2000) illustrates how macro- and micro-level institutions are related:

> . . . [M]arkets . . . are embedded in social institutions that guide behavior, involve organizations, that have internal structures (institutions) that guide behavior, and involve individuals making decisions in the context of market and organizational institutions and relationships.

3.2.7 Institutions Operating at Various Levels

Institutions influencing cyberattacks operate at different levels—global, national, local, social network, professional, industry, inter-organizational, and intra-organizational (Atkinson, 1991; Giddens, 1984; Kalipeni & Feder, 1999; Oppong & Kalipeni, 2005; Strang & Sine, 2002).

On institutions at the international/global level, Louis Henkin (1979) noted that "almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time." Thanks to globalization, governments are turning to supra-national institutions to resolve transnational problems (Smith & Wiest, 2005) such as cyberattacks. It should, however, be noted that although some commentators have argued that supra-national institutions are playing a crucial role in solving transnational problems (Dingwerth, 2005) and are reducing the power and autonomy of the state (Smith & Wiest, 2005), others have suggested that these institutions lack legitimacy as they lack a democratic mandate and have failed to represent broad interests (Castles, 2005).

Of greatest relevance here are national-level institutions—also known as the "country-level effects" or the "societal effects" (Zaheer & Zaheer, 1997)—which include political, legal, cultural, and other environmental factors specific to a country that influence cyberattacks. The state is arguably the most important external institutional actor and powerful drivers of institutional isomorphism since a violation of laws and regulations can have harsh economic and social sanctions (Bresser & Millonig, 2003).

At the industry/professional/inter-organizational level, external institutional actors exert pressure by threatening punishment in cases of noncompliance (Bresser & Millonig, 2003). Ethical codes of conduct set by different institutions and governing bodies such as professional associations and other private sector organizations are examples of institutions residing at inter-organizational level. The codes of conduct generally require members to maintain higher standards of conduct than required by law (Backoff & Martin, 1991).

At the societal network level, participants are encouraged to comply with the norms and values of the networks (Chung, 2004). A network can be defined as a group of "autonomous" actors "purposively involved in the group's activities" (Bieje & Groenewegen, 1992, p. 90). Some institutionalists refer traditional institutions consisting of custom and limited social networks (intragroup networks) of the pre-industrial era as the true forms of institutions (Sjostrand, 1992). Indeed, Gehlen (1957/1980) argued that modem society is being increasingly deinstitutionalized. In some societies, informal networks are still more effective than formal laws and regulations in dealing with local problems (Mol & Van Den Burg, 2004). An individual's social network is related to the obligation to be trustworthy and follow the norms of equity (Granovetter, 1985).

Different theoretical contributions and various empirical studies have led to the accepted view that that institutions within organizations or intra-organizational institutions have important consequences for organizations and their members including implementation of organizational knowledge and technology (Elsbach,

2002). These are associated with internal structures of organization (Deinhart, 2000). To take one example, in 2001, eBay announced a global ban on the sale of hate-related items on the company's websites (Wolverton, 2001).

3.3 Viewing Cybercrimes Through the Prism of the Literature on Institutions

The contexts of the economic activities were considered to influence the meaning and significance of institutions (Holm, 1995). In this chapter we consider formal and informal institutions from the standpoint of criminal activities.

3.3.1 Formal Constraints and Crimes

In prior literature, researchers have found organized crime groups thrive in a country with a weak state (Levi, 2002). Note that organized crime groups are increasing using the Internet to facilitate criminal activities (Finckenauer, 2005). The Italian Mafia, Japanese Yakuza, Chinese gangs, Colombian cartels, and Russian and Malaysian organized crime groups have reportedly employed hackers (Foreign Policy, 2005; Ismail, 2008; Katyal, 2001; Parker, 1998). The Business Software Alliance (BSA) urged US Congress to enact legislation to treat "cyber crime as organized crime" (Natividad, 2008).

A related concept is regulatory arbitrage, which exists when regulative institutions differ across countries in their permissiveness and conduciveness to crimes. Prior researchers have noted that transnational criminal groups' knowledge of regulatory variation in European countries allows them to use clever strategies to avoid prosecution (Levi, 2002). Likewise, financial frauds occur more in locations with less reporting obligations (Stewart, 2006).

3.3.2 Informal Constraints and Crimes

Studies of informal sanctions constitute a notable stream in the criminology literature. Prior researchers have noted the roles of informal psychological and social sanctions (e.g., shame, guilt, embarrassment, and rejection) in deterring socially undesirable and illegal behaviors (Aguilar-Millan et al., 2008; Blackwell, 2000; Clark & Davis, 1995; Paetzold, Dipboye, & Elsbach, 2008; Rasmussen, 1996; Smith, Simpson, & Chun-Yao, 2007). Proponents of "gay rights" legislation, for instance, argue that the real battle centers on gaining cultural acceptability and social legitimacy of such rights (Hu, 2001; Shilts, 1991) and stigmatizing "orthodox religious believers" (Duncan, 1994). Likewise, it is argued that culture and ethical attitudes may be a more crucial factor in driving software piracy than the level of economic development (Donaldson, 1996; Kwong et al., 2003).

Galtung (1958, p. 127) distinguishes two types of informal constraints facing a person (P): Institutionalized norms are "norms from other members from the social system to P" and internalized norms are "norms from P to himself." These are captured by Scott's (1995) normative and cognitive pillars. Institutionalized and internalized norms are related to external and internal stigma, respectively (Aguilar-Millan et al., 2008), which increase the psychic cost of feeling embarrassment and shame (Blackwell, 2000; Clark & Davis, 1995).

Institutionalized norms: Institutionalized norms are related to embarrassment, which is a socially imposed sanction that occurs when individuals violate norms endorsed by the society, especially by significant others (Blackwell, 2000; Paetzold et al., 2008). An external or social stigma is related to resentment against a criminal activity, which can lead to a deterrence of crimes (Rasmussen, 1996).

Prior researchers have also noted that from the society's point of view, whether crimes and victimization "elicit a stigma or a sympathy effect may depend on the evaluator's characteristics" (Lyons, 2006). The social identity theory points to the possibility of ethnocentric bias (Hamner, 1992; Tajfel & Turner, 1986). This means that ingroup victims and offenders are likely to be perceived sympathetically, while out-group ones may be stigmatized (Howard & Pike, 1986; Lyons, 2006). In a related vein, prior research also seems to indicate that racial prejudice leads to crimes (Hawkins et al., 1998).

Internalized norms: Internalized norms are related to internal stigma or a feeling of guilt and shame (Aguilar-Millan et al., 2008) and a negative evaluation of the self or a specific behavior (Harris, 2006; Lewis, 1971, 1992). Note that shame is a self-imposed sanction, which occurs as a reaction to individuals' violation of their internalize standards (Benedict, 1946; Freud, 1949/1930; Mead, 1937). Scholars also suggest that condemnation of a criminal act leads to internalization of norms against the act among the "condemners" and as well as the "condemned" (Kahan, 1996).

3.4 Institutions at Different Levels Influencing Cyberattacks

Table 3.1 illustrates how formal and informal institutions at different levels influence cyberattacks.

3.4.1 International-Level Institutions and Cyberattacks

Cyberattacks are global problems and for this reason, global-level institutions are likely to be effective to deal with such problems. As discussed in Chap. 1, supranational institutions such as International Telecommunications Union (ITU) and Interpol are working to strengthen regulative institutions related to cybercrime laws across the world.

Table 3.1 Institutions at different levels impacting cybercrimes

Level	Formal institutions	Informal institutions
Global/International	○ International laws and treaties	
National	○ National rules and laws	○ Political-normative views ○ Political-cognitive factors ○ Nationalism/patriotism-related hackings ○ National subculture and cybercrime patterns
Industry/profession/Inter-organizational		○ Pressure to deploy defense mechanisms (e.g., NASSCOM) ○ Engaging in cyberattacks to gain respect from peer hackers (e.g., red hackers)
Informal networks		○ Norms related to information sharing among hackers ○ Ideology: cyberattacks related to religion, fight against capitalism and nuclear proliferation, etc. ○ Cognitive legitimacy from parents and teachers
Intra-organizational		○ Norms related to reporting ○ Norms related to defense measures ○ Cognitive assessment of reporting cyberattacks

Given the global nature of cybercrime, fighting them more effectively would require global institutions with more effective compliance mechanisms. As are the cases of most global-level institutions and processes, international institutions designed to deal with cybercrime are, however, relatively underdeveloped. International treaties on cybercrime are weak and unenforceable.

3.4.2 National-Level Institutions and Cyberattacks

Compared to international institutions, the state arguably is more dominant in most areas of policy (Tarrow, 2001). National-level institutions provide a number of mechanisms to influence the cybercrime landscape.

Rules and laws: Cyberattack have benefited from jurisdictional arbitrage. Thanks to the newness, jurisdictional arbitrage is higher for cybercrimes compared to other conventional crimes. In a 2003 *Newsweek* article, Piore (2003, p. 48) argued that only the United States and the United Kingdom had "laws that come even close to adequate in defining cybercrimes and leveling penalties." The lack of a strong rule

of law is associated with the origination of more cyberattacks. A country with a strong rule of law is characterized by a strong court system and effective punishment and legal sanctions against criminals (Oxley & Yeung, 2001), which increase the expected probability of apprehension and conviction for criminals (see Eq. (2.1) in Chap. 2) (Ehrlich, 1996). A weak rule of law, on the other hand, is characterized by a lack of trust between the government and the citizens (Levi, 2002). Countries with weak rule of law and permissiveness of regulatory regimes thus provide a fertile ground for criminal activities (Mittelman & Johnston, 1999; Vassilev, 2003). Citizens' willingness to accept the established institutions and to obey the laws is equally important (The FBI Law Enforcement Bulletin, 2007).

Not surprisingly, organized cybercrimes are initiated from countries that have few or no laws directed against cybercrimes and little capacity to enforce existing laws (Grow & Bush, 2005; Williams, 2001). Eastern Europe and Russia's weak cybercrime laws have provided a fertile ground for computer crimes. Although many countries in Eastern Europe[2] have enacted cybercrime laws, they lack enforcement mechanisms.

A nation's laws also determine what is considered a cybercrime. For instance, in 2002, Germany announced that anyone promoting Holocaust denial, anywhere in the world, is liable under German law (Gabrys, 2002). Similarly, the Malaysian government announced that online insults to Islam would be punished (Perera, 2000).

National laws also facilitate or restrict law-enforcement agencies' ability to act on cybercrimes. In the United States, for instance, the FBI considers militant Islamist websites lawful as the First Amendment permits even the most hateful Internet speech, as long as they do not directly incite violence or raise money (Stephens, 2006). On the contrary, consider Singapore. In the cyber conflict with the Think Centre (Asia), an NGO, the state authorities reportedly employed surveillance and intimidation (Gomez, 2002, p. 76). There are reports that the government of Singapore actively scans and monitors e-mails and there are instances of breaking into a number of computers used by various groups and individuals (Gomez, 2002, pp. 43–44).

Law-enforcement agencies' responses also differ across types of cybercrimes. Experts argue that law-enforcement officials in some countries such as China and Russia do not take major actions against hackers attacking international websites and are more interested in protecting national security (Blau, 2004; Vardi, 2005).

Political cognitive factors: Mental maps of political elites or "persons who by virtue of their institutional positions have a high potential to influence national policy making" (Moore, 1979, p. 674) determine a nation's approach to cyberattacks. Political elites include legislators, governmental officials, political party officials, leaders of various interest groups, military leaders, etc.

An article published in *China Economic Times* on June 12, 2000 discussed three mechanisms that Xu Guanhua, then Chinese vice minister of the science and technology, thought high technology affects national security—military security, economic security, and cultural security. Regarding military security, Guanhua

forcefully argued that developed countries have put many hi-tech arms into actual battles and discussed the likelihood of ICT exporting countries installing software for "coercing, attacking or sabotage." Ironically, the truth or falsity of such claims is less relevant than the fear itself, which can significantly alter the equation of global security.

Some US observers, on the other hand, think that countries like China, Russia, and North Korea are systematically probing the computer networks in the United States to find weaknesses that can be exploited later (Bickers, 2001). A group of US defense analysts also argued that the growing use of Linux (open source software) in US defense systems presents an urgent national security threat. They have maintained that Linux companies have deployed development centers with programers from China and Russia, on one hand, and open nature of Linux enables hackers or cyber-terrorists to exploit the system, on the other hand. According to the US National Security Agency, some foreign governments have developed computer attack capabilities. Some US officials believe Iran, North Korea, Russia, and China have trained hackers in Internet warfare (Lenzner & Vardi, 2004). From the standpoint of national security, the truth or falsify of such fear is less relevant than the fear itself, which influences a nation's approach to deal with possible attacks on cyberinfrastructure and networks.

Political-normative effects: Political elites also differ on political-normative paths, which lead to variation to approaches to cybercrimes across nations. While there are government-backed cyber-terrorisms in some countries (Comité Européen Des Assurances, 2004), others have followed different approaches. A comparison of the United States and Burma illustrates this point. For instance, the United States has reportedly developed cyber-weapons capable of destroying an enemy's computer network, but there are disagreements about the appropriateness of employing such weapons (Adams, 2001). The Government of Burma, on the other hand, uses its advanced cyberwarfare department within the police force to track its online critics and sends virus-attached e-mails to exiled activists (Havely, 2000). A 2002 survey of Australian firms indicated that foreign governments were perceived as sources of attacks for 24% respondents (Deloitte Touche Tohmatsu, 2002).

National subculture and cybercrime patterns: Skorodumova (2004) provides a useful set of distinctions for characterizing hacking cultures associated with different nationalities. The American hackers, for instance, are characterized by personal motives such as self-advertising compared to Russians or Europeans. European hackers refrain from attacking well-known sites and advertising themselves. The US specialists believe that European hackers more often attack websites in protest or in defense of human rights. Likewise, Russian hackers see the authority and laws as hostile.

3.4.3 Institutions at the Industry/Professional/Inter-organizational Level and Cyberattacks

Some professional and trade associations can use social obligation requirements to induce certain behavior within organizations and the hacking community. There

are instances of professional and trade associations exerting isomorphic pressure to deploy appropriate defense measures. In India, the National Association of Software and Services Companies (NASSCOM) has played a critical role in the development of cybercrime-related institutions.

Motivation to earn respect from peer hackers also drives their actions. 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. The basis of compliance in such case thus derives from social obligations, and non-adherence can result in professional sanctions.

3.4.4 Institutions at the Network Level and Cyberattacks

Informal networks organized along a number of different lines also have values and norms that influence cyberattacks. First, consider families and broader social networks. There is some evidence that parents, and even teachers, advocate certain computer crimes, particularly software piracy among students (Bowker, 2000).

Other informal networks engaged in cyberinfrastructure, network, and computer attack spread across a wide geographical area. Some informal networks are organized along some type of ideology such as religion, fight against nuclear proliferation, and capitalism.

The networks of Islamic activists deserve special attention. 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.[3] Even more intriguing is the Society for Internet Research's finding which indicated that 70% of militant Islamist websites are hosted on computers based in the United States (Stephens, 2006).

Some act against the nation-state where they live. 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).

To take another example of ideological hacking, in June 1998, six hackers from the United States, the United Kingdom, the Netherlands, and New Zealand (identifying themselves as *Milworm*) hacked India's Bhabha Atomic Research Center's website (Denning, 2000). Similarly, in South Korea, 58 Internet servers were attacked by a Japanese student in November 2003 to protest the US-led war on Iraq (Duk-kun, 2003). 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.

Informal networks related to criminal organizations generally restrict membership according to various criteria such as ethnicity, kinship, race, and criminal background (Finckenauer, 2005) and in some cases corrupt public officials (Maltz, 1994, p. 27). The hawala system widely used in Middle East and Asia to move

money internationally, which also uses the Internet, relies on brokers linked by clan-based networks of trust (Homer-Dixon, 2002).

The hacking community is also characterized by a high degree of information sharing. Members in the community are willing to help fellow hackers to solve problems such as accessing a router and getting through a firewall (Bednarz, 2004). Typically, swapping and sharing of hacking tools and secrets take place in closed chat rooms (Acohido & Swartz, 2005).

3.4.5 Institutions at the Intra-organizational Level and Cyberattacks

Organizational idiosyncrasy may lead to varying responses to influences from the external environment (Zucker, 1991). The intra-organizational level is dominated by the normative component of institutions. An organization may voluntarily adhere to such norms, which may be subsequently internalized to be reflected in the organization's structures, strategies, and routines (Scott, 1995).

An important dimension of organizational norm related to cyberattacks is the organization's defense approach. We illustrate this point with Indian outsourcing firms' approach to prevent attacks on computers by current and former employees. In an attempt to address their clients' fear that customer data will be stolen and even sold to criminals (Lucas, 2004), Indian firms engaged in outsourcing have taken measures to prevent attacks on computers by current and former employees. For instance, call center employees have to undergo security checks which are considered to be "undignified" (The Economist, 2005). Firms have established biometric authentication controls for workers and banned cell phones, pens, paper, and Internet/e-mail access for employees (Fest, 2005). Computer terminals at Mphasis, an Indian outsourcing firm, lack hard drives, e-mail, CD-ROM drives, or other ways to store, copy, or forward data[4] (Engardio, Puliyenthuruthel, & Kripalani, 2004). Indian outsourcing firms also extensively monitor and analyze employee logs (Fest, 2005). Outsourcing firms in developing countries consider relationships with clients as important resources that can provide long-term returns on investment. To win and maintain legitimacy from their clients, structures and practices of Indian outsourcing firms have become non-isomorphic with respect to the local culture. Recall that organizations may engage in non-isomorphic responses if they perceive that such responses are likely to minimize a potential loss of resources (George et al., 2006).

To take another example, consider *The New York Times'* response after the company was duped into running a fake malware-loaded advertisement in September 2009. Following the security breach, the company suspended its practice of serving online ads directly from an advertiser's website (Kravets, 2009).

Organizations' cognitive assessment and norms related to reporting cyberattacks to authorities also influence law-enforcement agencies' ability to solve such crimes. As noted earlier, proportionally, much less cybercrimes than conventional crimes are reported to law-enforcement agencies.

3.5 Concluding Comments

The foregoing discussion provides a framework for understanding how institutions at various levels influence cyberattacks. An institutional perspective used in this chapter provides insights into factors and mechanisms that energize hackers' behaviors, nations' development, and deployment of cyber-weapons, law-enforcement agencies' responses to cyberattacks, organizations' defense mechanisms, and propensity to report cyberattacks on their networks, etc. From a theoretical perspective, our framework helps further explain patterns of cyberattacks.

As noted above, formal and informal institutions influence each other. Social and moral condemnation of cybercrime is thus likely to strengthen regulative institutions related to cybercrime. Likewise, legal system and legal discourse in relation to cybercrime are likely to influence social perception of cybercrimes.

Anti-cybercrime norms have not been fully institutionalized and internalized in the cyber-space. Institutions building efforts need to be carried out within the parameters of established culture, practices, discourses, power structures, and other institutions.

Notes

1. Deinhart (2000, p. xv) notes that "...business ethics is prescriptive while business and society is descriptive."
2. For instance, a law enacted in Romania in 2003 punishes convicts with up to 15 years in prison (Romania Gateway, 2003).
3. See "The rise of extremist hacking, criminal syndicates," http://star-techcentral.com/tech/story.asp?file=/2004/10/26/technology/9225925&sec=technology. Accessed 1 October 2009.
4. Since data theft is often committed by disgruntled former employees, Mphasis can lock an employee out and cut access to PCs and phones 3 minutes after a resignation. In 2003, the process took 3 days (Engardio et al., 2004).

References

Acohido, B., & Swartz, J. (2005, December 15). Meth addicts' other habit: Online theft. *USA Today*.

Adams, J. (2001). Virtual defense. *Foreign Affairs, 80*(3), 98–112.

Aguilar-Millan, S., Foltz, J. E., Jackson, J., & Oberg, A. (2008). The globalization of crime. *Futurist, 42*(6), 41–50.

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

Atkinson, A. (1991). *Principles of political ecology*. London: Belhaven Press.

Axelrod, R. (1997). *The complexity of cooperation*. New Jersey: Princeton University Press.

Backoff, J. F., & Martin, C. L., Jr. (1991). Historical perspectives: Development of the codes of ethics in the legal, medical and accounting professions. *Journal of Business Ethics, 10*, 99–110.

Baumol, W. J. (1990). Entrepreneurship: Productive, unproductive, and destructive. *Journal of Political Economy, 98*(5), 893–921.

Bednarz, A. (2004, November 29). Profiling cybercriminals: A promising but immature science. *Network World*. http://www.nwfusion.com/supp/2004/cybercrime/112904profile.html?page=2. Accessed 5 October 2006.

Benedict, R. (1946). *The chrysanthemum and the sword; Patterns of Japanese culture*. Boston: Houghton Mifflin.

Berger, P. L., & Luckmann, T. (1967). *The social construction of reality: A treatise in the sociology of knowledge*. New York: Doubleday.

Bickers, C. (2001). Combat on the web. *Far Eastern Economic Review, August 16*, 30–33.

Bieje, P.R., & Groenewegen, J. (1992). A network analysis of markets. *Journal of Economic Issues, 26*(1), 87–114.

Blackwell, B. S. (2000). Perceived sanction threats, gender, and crime: A test and elaboration of power-control theory, criminology. *Beverly Hills, 38*(2), 439–489.

Blau, J. (2004, May 26). Russia – A happy haven for hackers. http://www.computerweekly.com/Article130839.htm. Accessed 5 October 2006.

Bowker, A. L. (2000). The advent of the computer delinquent. *FBI Law Enforcement, 69*(12), 7–11.

Bresser, R. K. F., & Millonig, K. (2003). Institutional capital: Competitive advantage in light of the new institutionalism in organization theory. *Schmalenbach Business Review, 55*(3), 220–241.

Carson, S. J., Timothy, M. D., Grahame, R. D., & George, J. (1999). Understanding institutional designs within marketing value systems. *Journal of Marketing, 63*, 115–130.

Castles, S. (2005). Nation and empire: Hierarchies of citizenship in the new global order. *International Politics, 42*(2), 203.

Chung, K. H. (2004). Business groups in Japan and Korea: Theoretical boundaries and future direction. *International Journal of Political Economy, 34*(3), 67–98.

Clark, R., & Davis, W. L. (1995). A human capital perspective on criminal careers. *Journal of Applied Business Research, 11*(3), 58–64.

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 5 October 2006.

Davis, L., & North, D. C. (1971). *Institutional change and American economic growth*. Cambridge: Cambridge University Press.

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 5 October 2006.

Deinhart, J. W. (2000). *Business, institutions, and ethics*. New York: Oxford University Press.

Deloitte Touche Tohmatsu. (2002). *Australian computer crime and security survey.* http://www.4law.co.il/346.pdf. Accessed 5 October 2006.

Denning, D. E. (2000). *Acktivism: An emerging threat to diplomacy*. American Foreign Service Association. www.afsa.org/fsj/sept00/Denning.cfm. Accessed 5 October 2006.

Dingwerth, K. (2005). The democratic legitimacy of public-private rule making: What can we learn from the world commission on dams? *Global Governance, 11*(1), 65–83.

Donaldson, T. (1996). Values in tension: Ethics away from home. *Harvard Business Review, 74*(5), 48–57.

Dowling, J., & Pfeffer, J. (1975). Organizational legitimacy: Social values and organizational behavior. *Pacific Sociological Review, 18*, 122–136.

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

Duncan, R. (1994). Who wants to stop the church: Homosexual rights, legislation, public policy, and religious freedom. *Notre Dame Law Review, 69*, 393.

Ehrlich, I. (1996). Crime, punishment, and the market for offenses. *Journal of Economic Perspectives, 10*(1), 43–67.

Elsbach, K. D. (2002). Intraorganizational Institutions. *Blackwell Companion to Organizations*, 37–57.

Engardio, P., Puliyenthuruthel, J., & Kripalani, M. (2004, August 16). Fortress India? *Business Week, 3896*, 42–43.

Fest, G. (2005, September 1). Offshoring: Feds take fresh look at India BPOs; Major theft has raised more than a few eyebrows. *Bank Technology News, 18*(9), 1.

Finckenauer, J. O. (2005). Problems of definition: What is organized crime? *Trends in Organized Crime, 8*(3), 63–83.

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

Freud, S. (1949/1930). *Civilization and its discontents*. London: Hogarth Press and Institute of Psycho-Analysis.

Gabrys, E. D. (2002). The international dimensions of cyber-crime, Part 2. *Information Systems Security, 11*(5), 24–32.

Galtung, J. (1958). The social functions of a prison. *Social Problems, 6*, 127–140.

Gehlen, A. (1957/1980). *Man in the age of technology* (Reprint). New York: Columbia University Press.

George, E., Chattopadhyay, P., Sitkin, S. B., & Barden, J. (2006). Cognitive underpinnings of institutional persistence and change: A framing perspective. *Academy of Management Review, 31*(2), 347–385.

Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration*. Berkely, CA: University of California Press.

Gomez, J. (2002). *Internet politics: Surveillance and intimidation in Singapore.* Bangkok and Singapore: Think Centre (Asia).

Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. *American Journal of Sociology, 91*(3), 481–510.

Grasmick, H. G., & Robert, J. B. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law and Society Review, 24*, 837–862.

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

Hamner, K. M. (1992). Gay-bashing: A social identity analysis of violence against lesbians and gay men. In G. M. Herek & K. Berrill (Eds.), *Hate crimes: Confronting violence against lesbians and gay men* (pp. 179–190). Newbury Park, CA: Sage.

Harris, N. (2006). Reintegrative shaming, shame, and criminal justice. *Journal of Social Issues, 62*(2), 327–346.

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

Hawkins, J. D., Herrenkohl, T., Farrington, D. P., Brewer, D., Catalano, R., & Harachi, T. W. (1998). A review of predictors of youth violence. In R. Loeber & D. P, Harrington (Eds.), *Serious & violent juvenile offenders: Risk factors and successful interventions* (pp. 106–146). Thousand Oaks, CA: Sage.

Hayek, F. A. (1979). *Law, legislation and liberty* (3 vols.). Chicago: University of Chicago Press.

Henkin, L. (1979). *How nations behave.* New York: Council on Foreign Relations.

Hoffman, A. J. (1999). Institutional evolution and change: Environmentalism and the US chemical industry. *Academy of Management Journal, 42*(4), 351–371.

Holm, P. (1995). The dynamics of institutionalization: Transformation processes in Norwegian fisheries. *Administrative Science Quarterly, 40*(3), 398–422.

Homer-Dixon, T. (2002, January/February). The rise of complex terrorism. *Foreign Policy, 128*, 52–62.

Howard, J. A., & Pike, K. C. (1986). Ideological investment in cognitive processing: The influence of social statuses on attribution. *Social Psychology, 49*, 154–167.

Hu, V. T. (2001). Nondiscrimination or secular orthodoxy? Religious freedom and breach of contract at Tufts University. *Texas Review of Law & Politics, 6*(1), 289–333.

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

Jepperson, R. (1991). Institutions, institutional effects, and institutionalism. In W. W. Powell & P. J. DiMaggio (Eds.), *The new institutionalism in organizational analysis* (pp. 143–163). Chicago: University of Chicago Press.

Kahan, D. M. (1996). What do alternative sanctions mean? 63 U. *Chicago Law Review, 591*, 603–604.

Kalipeni, E., & Deborah, F. (1999). Environmental change in the Blantyre Fuelwood project area in Malawi: A political ecology perspective. *Politics and Life Sciences, 18*(1), 37–54.

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

Kelman, S. (1987). *Making public policy: A hopeful view of American government*. New York: Basic Books.

Kravets, D. (2009, September 14). New York Times reforms online ad sales after malware scam. *wired.com*. http://www.wired.com/threatlevel/2009/09/nyt-revamps-online-ad-sales-after-malware-scam/. Accessed 27 October 2009.

Kwong, K. K., Yau, O. H. M., Lee, J. S. Y., Sin, L. Y. M., & Tse, A. C. B. (2003). The effects of attitudinal and demographic factors on intention to buy pirated CDs: The case of Chinese consumers. *Journal of Business Ethics, 47*(3), 223–235.

Lenzner, R., & Vardi, N. (2004, September 20). The next threat. *Forbes, 174*(5), 15–21.

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

Lewis, H. B. (1971). *Shame and guilt in neurosis*. New York: International Universities Press.

Lewis, M. (1992). *Shame: The exposed self*. New York: Free Press.

Lucas, P. (2004). Outsourcing: The good, the bad & the ugly. *Collections & Credit Risk, 9*(12), 22–24.

Lyons, C. J. (2006). Stigma or sympathy? Attributions of fault to hate crime victims and offenders. *Social Psychology Quarterly, 69*(1), 39–60.

Macy, M. W., & Willer, R. (2002). From factors to actors: Computational sociology and agent-based modeling. *Annual Review of Sociology, 28*, 143–166.

Maltz, M. (1994). Defining organized crime. In R. J. Kelly, K.-L. Chin, & R. Schatzberg (Eds.), *Handbook of organized crime in the United States.* Westport, CT and London: Greenwood Press.

Mead, M. (1937). *Cooperation and competition among primitive peoples*. New York: McGraw-Hill.

Mittelman, J. H., & Johnston, R. (1999). The globalization of organized crime, the courtesan state, and the corruption of civil society. *Global Governance, 5*(1), 103–126.

Mol, A. P. J., & Van Den Burg, S. (2004). Local governance of environmental flows in global modernity. *Local Environment, 9*(4), 317–324.

Moore, S. (1979). The structure of a national elite network. *American Sociological Review, 44*, 673–691.

Natividad, K. F. (2008). Stepping it up and taking it to the streets: Changing civil and criminal copyright enforcement tactics. *Berkeley Technology Law Journal, 2008 Annual Review, 23*(1), 469–501.

North, D. C. (1990). *Institutions, institutional change and economic performance.* Cambridge, UK: Cambridge University Press.

North, D. C. (1994). Economic performance through time. *American Economic Review, 84*(3), 359–368.

North, D. C. (1996). Epilogue: Economic performance through time. In L. J. Alston, T. Eggertsson & D. C. North (Eds.), *Empirical studies in institutional change* (pp. 342–355). Cambridge, PA: Cambridge University Press.

Oppong, J. R., & Kalipeni, E. (2005). The geography of landmines and implications for health and disease in Africa: A political ecology approach. *Africa Today, 52*(1), 2–26.

Oxley, J. E., & Yeung, B. (2001). E-commerce readiness: Institutional environment and international competitiveness. *Journal of International Business Studies, 32*(4), 705–723.

Paetzold, R. L., Dipboye, R.L., & Elsbach, K. D. (2008). A new look at stigmatization in and of organizations. *Academy of Management Review, 33*(1), 186–193.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information.* New York: John Wiley & Sons, Inc.

Parto, S. (2005). Economic activity and institutions: Taking stock. *Journal of Economic Issues, 39*(1), 21–52.

Perera, R. (2000, November 26). Executives call for delay in cybercrime pact. *CNN.com*. http://www.cnn.com/2000/TECH/. Accessed 5 October 2006.

Piore, A. (2003, December 22). Computer Geeks: Hacking for dollars. *Newsweek International*. http://www.msnbc.msn.com/id/3706599/site/newsweek/print/1/displaymode/1098. Accessed 5 October 2006.

Rasmussen, E. (1996). Stigma and self-fulfilling expectations of criminality. *Journal of Law and Economics, 39*, 519–543.

Romania Gateway. (2003). Romania emerges as nexus of cybercrime. http://ro-gateway.ro/node/185929/comnews/item?item_id=223937. Accessed 5 October 2006.

Schneiberg, M., King, M., & Smith, T. (2008). Social movements and organizational form: Cooperative alternatives to corporations in the American insurance, dairy, and grain industries. *American Sociological Review, 73*(4), 635–667.

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. (1987). The adolescence of institutional theory. *Administrative Science Quarterly, 32*, 493–511.

Scott, R. (1995). *Institutions and organizations*. Thousand Oaks, CA: Sage.

Scott, R. (2001). *Institutions and organizations.* Thousand Oaks, CA: Sage.

Scott, W. R., Ruef, M., Mendel, P. J., & Caronna, C. A. (2000). *Institutional change and healthcare organizations: From professional dominance to managed care*. Chicago, IL: University of Chicago Press.

Shilts, R. (1991, January 1). The queering of America. *The Advocate*, 32–38

Sjostrand, S. E. (1992). On the rationale behind "irrational" institutions. *Journal of Economic Issues, 26*(4), 1007–1040.

Skorodumova, O. (2004). Hackers as information space phenomenon. *Social Sciences, 35*(4), 105–113.

Smith, T. (2003, October 27). Technology; Brazil Becomes a Cybercrime Lab. http://query.nytimes.com/gst/fullpage.html?res=9F02E3DA1131F934A15753C1A9659C8B63&sec=&spon=&pagewanted=2. Accessed 5 October 2006.

Smith, J., & Wiest, D. (2005). The uneven geography of global civil society: National and global influences on transnational association. *Social Forces, 84*(2), 621–651.

Smith, N. C., Simpson, S. S., & Chun-Yao, H. (2007). Why managers fail to do the right thing: An empirical study of unethical and illegal conduct. *Business Ethics Quarterly, 17*(4), 633–667.

Snidal, D. (1996). Political economy and international institutions. *International Review of Law and Economics, 16*(1), 121–137.

Stephens, H. (2006). Hosting Terror. *Foreign Policy, 155*, 92.

Stewart, J. (2006). White collar crime: Fraud, bribery and corruption—all alive and well? *Credit Control, 27*(4/5), 50–60.

Strang, D., & Sine, W. D. (2002). Interorganizational institutions. In J. Baum (Ed.), *Companion to organizations* (pp. 497–519). Oxford: Blackwell.

Tajfel, H., & Turner, J. C. (1986). The social identity theory of intergroup behavior. In S. Worchel & W. G. Austin (Eds.), *Psychology of intergroup relations* (pp. 7–24). Chicago, IL: Nelson-Hall.

Tarrow, S. (2001). Transnational politics: Contention and institutions in international politics. *Annual Review of Political Science, 4*, 1–20.

The Economist. (2005, September 10). Business: Busy signals; Indian call centres. *The Economist, 376*(8443), 66.

The FBI Law Enforcement Bulletin. (2007). Legitimizing criminal justice policies and practices, speech of Mark H. Moore as part of the Perspectives on Crime and Justice Series of the National Institute of Justice – Transcript.

Vardi, N. (2005, July 25). Chinese take out. *Forbes*, 54.

Vassilev, R. (2003). De-development problems in Bulgaria. *East European Quarterly, 37*(3), 345.

Webb, J. W., Tihanyi, L., Ireland, R. D., & Sirmon, D. G. (2009). You say illegal, I say legitimate: Entrepreneurship in the informal economy. *Academy of Management Review, 34*(3), 492–510.

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 5 October 2006.

Wolverton, T. (2001, November 8). Court shields Yahoo from French laws. *CNET News*. http://news.cnet.com/2100-1017-275564.html. Accessed 5 October 2006.

Zaheer, S., & Zaheer, A. (1997). Country effects on information seeking in global electronic networks. *Journal of International Business Studies, 28*(1), 77–100.

Zucker, L. (1991). The role of institutionalization in cultural persistence. In W. W. Powell & P. J. DiMaggio (Eds.), *The new institutionalism in organizational analysis* (pp. 83–107). Chicago: University of Chicago Press.