Chapter 5
Institutional Field Evolved Around Cybercrimes

> *"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" (a carder in Indonesia, Antariksa, 2001, p. 16).*
>
> *"Trust in Nigerian businessmen and princes" is among the "50 things that are being killed by the internet" (*Telegraph.co.uk, *4 September 2009, Moore, 2009).*

Abstract The growth of criminal enterprises in the cyberworld has been an issue of pressing concern to our society. Concepts and theory building are lacking on institutions from the standpoint of criminal entrepreneurship in the digital world. In an attempt to fill this void, this chapter proposes a framework for identifying clear contexts and attendant mechanisms associated with how institutions have interacted with cybercrimes. The underlying notion in this chapter is that the rules of the game offered by formal and informal institutions have favored cybercrimes more than most conventional crimes. The degree of institutional favor, which cybercrime-related entrepreneurs enjoyed before, however, is decreasing.

5.1 Introduction

It is apparent that, from the standpoint of the cybercrime industry, institutions have changed dramatically in the past few decades. There has been "historical and cultural shifts in practices, discourses and representations of hacking" (Best, 2003). In the 1960s, the term "hacker"[1] referred to a person able to solve technologically complex problems (Furnell, Dowland, & Sanders, 1999). As late as the 1980s, "hackers" were considered to be people with high level of computing skills. A complaint that was often heard in the law-enforcement community was that some hackers were "treated as media darlings" (Sandberg, 1995). Until the 1980s, there were a few laws to tackle hacking and cybercrimes. The Computer Fraud and Abuse Act, for instance, was one of the first laws developed to deal with cybercrimes (Table 5.1). The act was originally passed in 1984 to protect classified

N. Kshetri, *The Global Cybercrime Industry*, DOI 10.1007/978-3-642-11522-6_5,

information on government computers, which was broadened in 1986 to apply to "federal interest computers" (Davis, 2006).

In the past few decades, the fields of hacking and cybercrime have undergone political, social, and psychological metamorphosis. Cybercrime has been recognized as a mainstream crime. For instance, starting 2009, Gallup included identity theft as a category in its annual survey to study Americans' fear of being crime victims (Saad, 2009). Nowadays, hackers are often portrayed in the popular press

Table 5.1 Major events related to the evolution of cybercrime-related institutions

1973	Swedish Data Act of 1973 was enacted
1977	Senator Abe Ribicoff introduced the "Federal Computer Systems Protection Act of 1977". This was the first proposal for Federal computer crime legislation in the United States. The Bill was not adopted, but became the model legislation in state computer crime legislation[a]
1981	Interpol became the first international organization dealing with computer crimes
1981	Tracy Kidder's The Soul of a New Machine published
1982	Hollywood film Tron released
1983	The OECD appointed an expert committee to discuss computer-related crime
1983	Hollywood film Wargames released
1984	The Computer Fraud and Abuse Act was passed to protect classified information on government computers
1984	Steven Levy's "Hackers: Heroes of the Computer Revolution" published
1985	The CoE appointed an expert committee to discuss legal issues of computer crimes
1986	The Computer Fraud and Abuse Act was broadened to apply to "federal interest computers"
1989	The CoE recommendations addressing the need for new substantive laws criminalizing certain conduct committed through computer networks (Recommendation No. R. (89) 9)
Nov. 1989	Masters of Deception group attacked the Learning Link computer system operated by WNET, Channel 13, in New York
1990	The UN adopted a resolution on computer crime legislation at 8th UN Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba, in 1990
1992	Wurzburg conferences organized by the University of Wurzburg led to 29 national reports, and recommendations for the development of computer crime legislations
1994	The United Nations Manual on the Prevention and Control of Computer was developed
1995	Hollywood film Hackers released
1995	The CoE recommendations concerning problems of criminal procedure law related to IT
1996	The Computer Fraud and Abuse Act was replaced by the more general concept of "protected computer," making the statute more widely applicable to the private sector
1997	CoE Committee of Experts on Crime in Cyber-space was set up
1999	The first conviction under the NET Act
2000	A Philippino hacker launched the "Love Letter" virus
Mar. 2000	The US Department of Justice opened www.cybercrime.gov
Oct. 2001	The USA Patriot Act was enacted to expand the intelligence gathering and surveillance powers of law-enforcement and national security agencies

Table 5.1 (continued)

Nov. 2001	34 countries signed the CoE's Convention on cybercrime
2002	Cybercrime and cyber-terrorism became FBI's No. 3 priority
July 2002	The Gramm-Leach-Bliley Act of 1999 went into effect. It requires financial institutions to establish procedures for protecting personal information, including. Financial penalties and civil suits may result from the inadvertent disclosure of personal information[b]
Nov. 2002	Cybersecurity Enhancement Act of 2002 signed
Apr. 2004	Computer Software Privacy and Control Act signed
Nov. 2007	The Identity Theft Enforcement and Restitution Act of 2007 enacted
May 2009	US President Obama created a new White House office led by a Cybersecurity Coordinator
Oct. 2009	Gallup included identity theft in its annual survey conducted to study trends of Americans' fear of being crime victims[c]

[a] A brief history of computer crime legislation, http://www.cybercrimelaw.net/content/history.html
[b] http://www.allshredservices.com/faq/grammleachbliley.htm
[c] Saad (2009).

as "criminal, deviant and disorderly" (Best, 2003). Many sub-groups related to "hacker" are considered to be socially undesirable (Furnell et al., 1999). On the political front, many laws are enacted to deal with the rapidly growing cybercrimes. For instance, in 1996, the Computer Fraud and Abuse Act was replaced by the more general concept of "protected computer," making it widely applicable to the private sector (Table 5.1). Likewise, the US Patriot Act brought cyberattacks into the definition of terrorism with penalties of up to 20 years in prison. As of 2006, over 30 US states had laws that require businesses to report cybercrimes (Greenemeier, 2006).

How did the transformations occur in institutions related to hacking and cybercrime? Why is cybercrime rising despite the institutional transformations? These questions are not idiosyncratic to the cybercrimes, but pertain to an under-researched subject in institutional theory: What factors influence the legitimacy of a criminal activity? How do institutions related to such an activity change? It is important to note that an important and long-standing question in institutional research is how institutional change occurs (Greenwood, Suddaby, & Hinings, 2002). A related point is that "how existing logics and identities are dismantled and how actors adopt a new logic and identity" has been an under-researched aspect of institutional theory (Rao, Monin, & Durand, 2003). In this chapter, we seek to understand the loci of institutions related to cybercrimes in order to understand the growth of and institutional changes related to such crimes.

5.2 The Theoretical Framework: Institutional Field

The idea of institutional field can be very helpful in understanding institutions and institutional changes associated with cybercrimes. A field is "formed around the issues that become important to the interests and objectives of specific collectives of organizations" (Hoffman, 1999, p. 352). For a field formed around cybercrimes, these organizations include regulatory authorities, international organizations (e.g., WTO, The Council of Europe (CoU)), and software producers. The "content, rhetoric, and dialogue" among these constituents influence the nature of field formed around cybercrime (Hoffman, 1999, p. 355).

Institutional fields are "evolving" rather than "static" in nature (Hoffman, 1999, p. 352). Institutional theorists make an intriguing argument as to how a field evolves. A field is a dynamic system characterized by the entry and exit of various players and constituencies with competing interests and disparate purposes and a change in interaction patterns among them (Barnett & Carroll, 1993). As is the case of any "issue-based" field, these players continuously negotiate over issue interpretation and engage in institutional war leading to institutional evolution (Greenwood & Hinings, 1996).

Prior researchers have noted that fields evolve through three stages (Morrill, 2007, cf. Purdy & Gray, 2009). New logics are introduced and are drawn into debate in the innovation stage, which is the first stage of field evolution. In the second stage, mobilization, field development is characterized by a complex power dynamics. Institutional actors in this stage compete to validate and implement their logics. The final stage is the structuration stage, in which logics are translated into practices (Reay, Golden-Biddle, & GermAnn, 2006). In this stage, norms and structures are standardized and institutions deepen their taken-for-grantedness (Covaleski & Dirsmith, 1988; DiMaggio, 1991).

Prior research also indicates that institutional evolution entails transitions among the three institutional pillars—regulative, normative, and cognitive. Building a regulative/law pillar system is the first stage of field formation. It is followed by a formation of normative institutions (cybercrimes' assessment from ethical viewpoint) and then cognitive institutions ("culturally supported belief" related to cybercrimes) (Hoffman, 1999).

The formation of regulative pillar is characterized by the establishment of legal and regulatory infrastructures to deal with cybercrimes (Hoffman, 1999). The strength of this pillar also depends upon the state's administrative capacities and citizens' willingness to accept the established institutions. A normative institutional pillar is said to be established regarding cybercrime if such a crime is viewed as an ethically and socially inappropriate behavior. Likewise, a cognitive pillar related to cybercrime is established if there is a culturally supported belief that cybercrime is wrong.

In a discussion of institutional field around cybercrime the nature of social stigmatization (Blackwell, 2000; Grasmick & Bursik, 1990; Probasco, Clark, & Davis, 1995) deserves special attention. From the standpoint of stigmatization of cyber-criminals, to understand the roles of players and constituencies related to field formed around cybercrime, a central concept here is arbiter. Drawing on the conceptual foundation provided by theories of socially situated judgment (Bell & Tetlock, 1989; Kahneman, 2003; Tetlock, 2002), Wiesenfeld, Wurthmann, and Hambrick (2008) argue that arbiters' "constituent-minded sensemaking" influences stigmatization process. Wiesenfeld et al. (2008) have identified three categories of "arbiters"— social, legal, and economic. Social arbiters include members of the press, governance watchdog groups, academics, and activists. Legal arbiters are those who play role in enforcing rules and regulations. Economic arbiters make decisions about engaging in economic exchange with individuals.

Legal arbiters, who enforce rules, have stepped up campaign against cybercrimes. The Federal Trade Commission (FTC), the DOJ, and the Department of Homeland Security have taken measures to create public awareness of cybercrimes and to improve cyber readiness.

Social arbiters include members of the press, governance watchdog groups, academics, and activists. The media's anti-cybercrime sentiments are reflected in their negative discourses of criminal hackers (Best, 2003). Academics and activists have also pointed out that software vendors should not expect consumers to create their own security software and bear liability for cybercrimes (Ryan, 2003; Rustad & Koenig, 2005). Religious groups can also be considered as social arbiters. In June 2009, for instance, the Head Pastor of a Christian Centre in Ghana urged Pastors, and Christians in general, to declare war against cyber-fraud also known as "sakawa" (ghanabusinessnews.com, 2009). He made the call at a special prayer session, which was organized by the Church for the nation against the spread of cybercrime.

Economic arbiters make economic exchange-related decisions. In this regard, businesses are actively mobilizing discourses against technology and service providers to take anti-cybercrime measures. In 2006, a coalition of major brands such as Expedia and LendingTree expressed dissatisfaction with click fraud and pressured Google and Yahoo to be more accountable (Grow & Bush, 2005).

A field is a dynamic system characterized by the entry and exit of various members and constituencies with competing interests and disparate purposes and a change in interaction patterns among them (Barnett & Carroll, 1993). For a field formed around cybercrime, the members include criminal hacker (also known as black hat hackers), ethical hackers (or white hat hackers), regulatory authorities (e.g., the FBI), international organizations (e.g., Council of Europe and the G8 High Tech Crime Working Group), software manufacturers, and consumers. As is the case of any issue-based field, these field members continuously negotiate over issue interpretation and engage in institutional war, leading to institutional evolution (Barnett & Carroll, 1993; Hoffman, 1999). The "content, rhetoric, and dialogue" among the field members influence the nature of cybercrime and institutionalization of anti-cybercrime logics (Hoffman, 1999, p. 355).

Various members in an institutional field differ in their influence in shaping the field. The dominant field members, for instance, tend to be those with "greater formal authority, resources and discursive legitimacy" (Phillips, Lawrence, & Hardy, 2000, p. 33). A field member's degree of dominance is positively related to the member's influence in the development of the field's structures and practices (Phillips et al., 2000).

5.3 Institutional Field Change Mechanisms

To understand the changes in formal and informal constraints related to cybercrime, it may be helpful to consider a set of institutions, including practices, understandings, and rules; as well as a network of related organizations (Tolbert & Zucker, 1983). In this regard, it is important to note that in looking at issues of institutional development and change from the standpoint of cybercrime, we are treating institutions as endogenous. Doing so, however, requires an understanding of other "higher" level existing institutions and exogenous parameters (Snidal, 1994, 1996). Snidal (1996, p. 131): "In the short run, given exogenous institutional and other constraints, actors maximize their outcomes both through their behavior and through the development of efficient endogenous institutions. In the longer term, exogenous institutional constraints are themselves subject to change. There may be efficiency gains in changing these erstwhile exogenous institutions as well as the corresponding endogenous institutions."

In prior theoretical and empirical research, scholars have identified mechanisms related to changes in institutional fields: "jolts" or exogenous shocks (Meyer, 1982; Meyer, Brooks, & Goes, 1990; Haveman, Russo, & Meyer, 2001; Meyer, Gaba, & Colwell, 2005), changes in organizational logics (Friedland & Alford, 1991; Leblebici, Salancik, Copay, & King, 1991; Haveman & Rao, 1997; Thornton & Ocasio, 1999), and gradual change in field structure (Clemens & Cook, 1999; Fligstein, 1991; Schneiberg, 2005).

5.3.1 Exogenous Shocks

According to Hoffman's (1999) model, evolution of an institutional pillar is associated with and facilitated by initiating events or triggers also known as disruptive events. Disruptive events are also referred to as shocks (Fligstein, 1991), jolts (Meyer, 1982), or discontinuities (Lorange, Scott, & Ghoshal, 1986) and can overcome the effects of institutional inertia (White, 1992).

Disruptive events tend to create "disruptive uncertainty" and force organizations to adopt "unorthodox experiments" that differ drastically from established practice (Meyer, 1982). Preliminary evidence consistent with this proposition emerges from some governments' responses to cybercrimes. New forms of major cybercrimes have led to new laws as well as the creation of technical infrastructure for monitoring and tracing (Katyal, 2001). According to Hannigan's (1995) typology, these disruptive events can be considered as catastrophes[2] in the cyberworld. For instance, in 2000, following hackers' attacks of several major websites, the US Congress considered proposals to improve security (Morning Edition, 2000). In March 2000, the US Department of Justice (DOJ) opened the website: www.cybercrime.gov. The site provided measures to protect against hackers and to report cybercrimes (New York Times, 2000). Others materials featured on the website include DOJ reports and speeches, congressional testimony, efforts to protect infrastructures, and international efforts on that front (Larkin, 2000).

Similarly, following the September 11 attacks, the USA Patriot Act was enacted in 2001 to expand the intelligence gathering and surveillance powers of law-enforcement and national security agencies. As noted earlier, cybercrime and cyber-terrorism also became FBI's No. 3 priority since 2002.

Likewise, after a Philippino hacker launched the "Love Letter" virus in 2000, the Philippine Republic Act 8792 was enacted. The electronic commerce act laid out how "hacking or cracking" crimes should be punished in the country (Evans, 2000). Legal and administrative happenings also act as disruptive events (Hannigan, 1995). In 2007, New York State held advertisers responsible for using an agency distributing adware, which changed advertisers' adware policies.

5.3.2 Changes in Organizational Logics

In prior theoretical and empirical research, scholars have emphasized the coevolving nature of institutions and the organizational forms that embody them and found that changes in organizational logics lead to a change in a field's practices and conventions (Friedland & Alford, 1991; Leblebici et al., 1991; Haveman & Rao, 1997; Thornton & Ocasio, 1999). In a study of the thrift industry, Haveman and Rao (1997, p. 1614) found that creation of new organization and adoption of structures embodying norms, value, and beliefs lead to an expansion of institutional influences. Destruction of organizational infrastructures, on the other hand, is associated with the decline of institutions (Haveman & Rao, 1997).

There have been changes in organizational logics at various levels. First, consider government agencies. In 2006, the FBI and the US Postal Inspection Service realized that click fraud may have violated federal laws. There have also been changes in the logics of trade associations. In 2006, the Internet Advertising Bureau (IAB) launched the Click Measurement Working Group to create Click Measurement Guidelines including definition of a click, standard to measure and count clicks, and identify invalid clicks. Individual organizations have also changed their structures and practices. In 2006, Priceline stopped utilizing adware providers and adopted best practices related to Internet ads.

5.3.3 Gradual Change in Field Structure

Structure of an institutional field may change over time with the changes in rules and norms governing the field. Cybercrime-related institutions and related organizations have also undergone gradual changes. Observers have noted "historical and cultural shifts in practices, discourses and representations of hacking" (Best, 2003). In the 1960s, for instance, the term "hacker" referred to a person able to solve technologically complex problems (Furnell et al., 1999). As late as the 1980s, "hackers" were considered to be people with superior computing skills. A complaint that was often heard in the law-enforcement community was that some hackers were "treated as media darlings" (Sandberg, 1995). As noted earlier, the media nowadays is mostly against hackers. Many sub-groups related to "hacker" are considered to be socially undesirable (Furnell et al., 1999).

The nature of gradual change in field structure can also be explained with the entry and exit of field members and relative power and dominance of various members in the field. In this regard, an issue that deserves mention relates to the government agencies' increasing power and dominance through formal authority and resources. Likewise, the entry of cybercrime-related supranational organizations such as Council of Europe and the G8 High Tech Crime Working Group has a powerful impact on institutional fields formed around cybercrime at the national level.

Regulative agencies' structures to fight cybercrime have also changed. In 1996, the FBI established Computer Investigations and Infrastructure Threat Assessment Center, which grew to 1,151 employees in 2007.

5.4 Institutional Evolution

Prior research indicates that institutional evolution entails a sequence of evolutionary development among the three institutional pillars—regulative, normative, and cognitive. Building a regulative/law pillar system is often the first stage of field formation. According to Hoffman (1999), it is followed by the formation of normative institutions (cybercrime as an ethically inappropriate behavior) (p. 363) and then cognitive institutions ("culturally supported belief" against cybercrime) (p. 364).

5.4.1 Regulative Pillar Related to Cybercrime

Regulative institutions consist of regulatory bodies (such as the FBI) and existing laws and rules related to cybercrimes. The formation of this pillar is characterized by the establishment of legal and regulatory infrastructures to combat cybercrimes (Hoffman, 1999). The strength of this pillar also depends upon the state's administrative capacities and citizens' willingness to accept the established regulative institutions.

5.4.2 Normative and Cognitive Pillars Related to Cybercrime

Responses to external pressures are functions of a social construction. Normative constraints discourage actions as "negative sanctions are anticipated if the actions are carried out" (Galtung, 1958; p. 127). Galtung (1958, p. 127) distinguishes two types of normative 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" (p. 127). These norms can be expressed in the forms of shame and embarrassment. Psychic costs associated with shame and embarrassment reduces the propensity to commit a crime (Blackwell, 2000; Probasco et al., 1995). Shame is a "self-imposed sanction," which occurs when individuals violate their internalized norms (Grasmick & Bursik, 1990). Embarrassment, on the other hand, is related to a "socially imposed sanction" that occurs when actors violate norms that have been endorsed by others in the society (Probasco et al., 1995). Put differently, embarrassment is related to social stigmatization (Blackwell, 2000).

The formation of an anti-cybercrime institutional field requires the construction of new identities that redefine social, cognitive, and moral legitimacy related to cybercrime; frame actions in an anti-cybercrime manner; and facilitate the development of habits and practices consistent with an anti-cybercrime logic (Misangyi, Weaver, & Elms, 2008).

An anti-cybercrime normative pillar is said to be established if cybercrime is viewed as an ethically inappropriate behavior and institutional actors feel a sense of social obligation to act against cybercrimes. Likewise, an anti-cybercrime cognitive pillar is established if there is a culturally supported belief that cybercrime is wrong (Hoffman, 1999). Measures taken to build normative and cognitive pillars should affect both substance as well as symbolism related to cybercrime (Misangyi et al., 2008).

5.5 Institutional Field Formed Around Cybercrimes

5.5.1 The Formation of Regulative Pillar Around Cybercrime

A central concept here is related to dominant field members. The idea of the government in a country as a dominant field member can be very helpful in understanding the development of regulative institutions. Prior research indicates that powerful and dominant field members tend to be those with "greater formal authority, resources and discursive legitimacy" (Phillips et al., 2000, p. 33; Hardy & Phillips, 1998).

Formal authority is related to an institutional actor's "legitimately recognized right to make decisions" (Phillips et al., 2000, p. 33). In most cases, such power lies with the government (Hardy & Phillips, 1998). While new cybercrime laws have increased the government's formal authority in industrialized countries, many developing countries have no laws dealing with cybercrimes. In 2000, for instance, only about 45 nations in the world had laws recognizing and validating some forms of digital or electronic transactions (Kshetri & Dholakia, 2001). This means that even if governments in some developing countries want to fight against cybercrimes, a lack of regulatory framework means that they lack formal authority to do so.

Industrialized countries have also increased resources[3] devoted to fight cybercrimes. While some maintain that resources to fight cybercrimes are far from sufficient in industrialized countries, there has been a greater achievement in these countries than in developing countries. Many developing economies, on the other hand, lack resources to build anti-cybercrime institutions (Cuéllar, 2004). As one might expect, developing countries lack judges, lawyers, and other law-enforcement workforce, who understand cybercrimes.

Discursive legitimacy concerns speaking legitimately about issues and affected organizations (Phillips & Brown, 1993). Undoubtedly, increased cybercrimes in developed countries such as the United States has helped gain discursive legitimacy for agencies involved in anti-cybercrime efforts. To gain discursive legitimacy, www.cybercrime.gov, for instance, featured DOJ reports and speeches, congressional testimony, efforts to protect infrastructures, and international efforts on that front (Larkin, 2000). All this has to be contrasted with situations in developing countries, where governments lack discursive legitimacy to take actions against cybercrimes. Consider, for instance, piracy, a form of cybercrime. In developing countries, consumers perceive anti-piracy enforcement tools as supports to foreign software companies. The Taiwanese government's attempt to force students using pirated versions of Windows to pay up was perceived as a support to a foreign company rather than its own citizens (Kshetri, 2004). In sum, most governments in developing countries have been unable to fight cybercrimes due to the lack of resources, formal authority, and discursive legitimacy.

In sum, an increase in cybercrimes in a country leads to the development of stronger regulative institutions. A lower income country is thus likely to have thinner and more dysfunctional regulative institutions related to cybercrimes than a higher income country.

5.5.1.1 National and International Initiatives to Build Strong Regulative Institutions

Supranational institutions such as International Telecommunication Union (ITU) and the Council of Europe (CoU) are influencing individual countries to strengthen cybercrime-related regulative institutions. As of August 2009, 46 nations had signed the CoE Treaty and 26 of them ratified it (Chap. 1).

Many governments want to strengthen their countries' anti-cybercrime institutions. For instance, China is facing unprecedented political and trade pressures from Western governments to combat cybercrimes. Consequently, in contrast to the 1980s, China's central government leaders do not ignore or promote piracy and other forms of cybercrimes (Massey, 2006).

People's compliance and cooperation with regulatory requirements, however, are driven largely by their belief in the legitimacy and fairness of legal authority rather than the fear of remedial measures and sanctions (Balganesh, 2008). Hart (1961) referred this idea as the "critical reflexive attitude." For instance, consumers in Taiwan perceived the government's anti-piracy efforts unfair as they viewed the efforts as support to foreign software companies rather than its own citizens.

5.5.1.2 Higher Cybercrime Level Leading to Strong Regulative Institutions

An observation is that an increase in cybercrime victimization may strengthen anti-cybercrime regulative institutions through various institutional change mechanisms such as exogenous shocks (Meyer, 1982), changes in organizational logics (Friedland & Alford, 1991), and gradual change in institutions (Clemens & Cook, 1999). There are three interrelated reasons why a higher level of cybercrime victimization strengthens anti-cybercrime institutions. First, the government faces pressures to improve anti-cybercrime regulatory institutions and infrastructures. In the US, for instance, the Business Software Alliance (BSA) urged the Congress to enact legislation to "treat cybercrime as organized crime" and increase penalties (Natividad, 2008).

Second, a high-cybercrime level serves as a basis for the theorization process, which is an important stage in institutional change (Greenwood et al., 2002). Theorization provides rationales for the practices and thus increases the likelihood of acceptance of the practice (Strang & Meyer, 1993). Two key elements of theorization concern framing and justifying. Framing focuses on the need for change and justification is value of the proposed changes for concerned actors (Greenwood et al., 2002; Maguire, Hardy, & Lawrence, 2004). Businesses and governments may use increased cybercrime victimization as a basis for justifying actions to change established practices.

Regulators expanding their scope: Regulatory measures have been expanded in recent years in order to provide more comprehensive coverage of a diverse range of economic activities. Due to the increased concerns about cybercrimes, the Committee on Foreign Investment in the United States (CFIUS) regulations have been changed to protect the US company. According to new CFIUS regulations, a potential foreign acquirer of a US company needs to certify the cybersecurity protections that will be in place with respect to the acquired US company (Asner & Kleyna, 2009).

Finally, as noted in Chap. 1, when businesses are victimized, they are likely to help develop anti-cybercrime regulative institutions by pursuing cyber-criminals under the existing laws. For instance, in 2009, as allowed under the CAN-SPAM Act,[4] Facebook sought damages of over $7 billion from Sanford Wallace. A California federal judge awarded Facebook US $711 million (Claburn, 2009). Sanford Wallace also owed MySpace $234 million from another judgment in another suit.

5.5.1.3 Political Institutions' Built-In Biases Toward Manufacturers of Technologies

Drawing on political resource theory (Hicks, 1999), institutional politics theory (Amenta, 1998) and power constellations theory (Huber & Stephens, 2001), Jenkins, Leicht, and Wendt (2006) point to the possibility that "political institutions have built-in biases that systematically favor the interests of specific classes." State policy can be viewed as "the result of power relations in society mediated by political institutions" (Huber & Stephens, 2001, p. 13) or "a joint product of class forces and political institutions" (Jenkins et al., 2006). Commenting on the government's ability to develop capacity to fight crimes, Cuéllar (2004) notes: "building capacity may require regulatory enforcement and programs that are costly to certain interest groups" (p. 45). In this regard, one important aspect of cybercrime that renders it interesting is the fact that laws in industrialized countries do not require manufacturers of technologies to assume responsibility for the faults in their products (e.g., software flaws) (Bank, 2005). A *USA Today* article (2002) put the issue this way: "For decades, software makers have been protected from lawsuits as US courts have struggled with the task of defining something as abstract and fast-changing as computer code." The UK House of Lords' *Personal Internet Security* report published in 2007 stated: "The IT industry has not historically made security a priority" (IAM, 2007).

5.5.1.4 Arbiters and Institutional/Social Entrepreneurship

In recent years, different groups of arbiters are moving beyond cyber-criminals and are targeting groups that have enabled cybercrimes. Liability issues associated with network security have received considerable attention (Mead, 2004). For instance, the prospect of software vendor liability is gaining speed. Social arbiters such as watchdog groups, academics, and activists have pointed out that software vendors should bear liability for cybercrimes. Some experts argue that software vendors should not expect consumers to create their own security software (Ryan, 2003). Rustad and Koenig (2005) argued that software vendors should be liable to consumers for a new tort—the negligent enablement of cybercrime. Similarly, National Academy of Sciences (NAS) argued that companies producing insecure software should be punished and the congress should take actions on this front (Computer Fraud & Security, 2002). NAS wrote in a draft report on the nation's computer security systems after the September 11, 2001 attacks: "Policy makers should consider legislative responses to the failure of existing incentives to cause the market to respond adequately to the security challenge . . . . Possible options include steps that would increase the exposure of software and system vendors and system operators to liability for system breaches." Economic arbiters such as government and private sector CIOs, on the other hand, have suggested imposing sanctions on vendors whose software is breached (Miller, 2002).

The concepts of social entrepreneurship and institutional entrepreneurship can be helpful to understand the roles of these arbiters. Social entrepreneurs (e.g., NAS and academics) are individuals or private organizations, whose entrepreneurial behaviors are engaged in addressing social problems (Korosec & Berman, 2006; Wong & Tang, 2006/2007, p. 627). Institutional entrepreneurs "help establish market institutions in the process of their business activities" (Daokui Li, Feng, & Jiang, 2006, p. 358). DiMaggio (1988, p. 14) notes that "new institutions arise when organized actors with sufficient resources (institutional entrepreneurs) see in them an opportunity to realize interests that they value highly." They champion a model of social order and attempt to build new organizational fields to institutionalize that model (Bartley, 2007). Government and private sector CIOs in the above discussion can be considered as institutional entrepreneurs.

In response to pressures from social and institutional entrepreneurs, regulators have also taken some measures, at least symbolic, to make software vendors responsible for cybercrimes. The UK House of Lords' Personal Internet Security report published in 2007, for instance, called for "software vendors (to) make the development of more secure technologies their top design priority" (IAM, 2007).

5.5.2 The Formation of Normative Pillar Around Cybercrime

Condemnation of an act such as a cybercrime leads to internalization of norms against the act among the "condemners" and as well as the "condemned" (Kahan, 1996). From the society's point of view, whether victimization related to a crime "elicit a stigma or a sympathy effect may depend on the evaluator's characteristics" (Lyons, 2006). In this regard, social identity theory points to the possibility of ethnocentric bias (Hamner, 1992; Tajfel & Turner, 1986).

A central tenet of social identity theory is that ingroup victims and offenders are likely to be perceived sympathetically, while out-group victims and offenders may be stigmatized (Howard & Pike, 1986; Lyons, 2006). We extend this logic to argue that as more and more individuals and organizations experience cyberattacks and they belong to the ingroup of cybercrime victim, anti-cybercrime societal norms are likely to be stronger. On a more speculative basis, we can argue that Mitnick's hacking activities is more likely to be perceived in a negative way today compared to the mid-1990s.

A related point is that, the perceived social stigma associated with becoming a cybercrime victim may also reduce with an increase in cybercrime. Note that most Internet fraud victims are embarrassed to report that they have been victimized (Salu, 2004).

To illustrate this argument, we consider the transformation in cybercrime-related societal norms. Until the mid-1990s, cyber-criminals in the United States lacked social stigma. A US attorney argued that the public was impressed because cybercrime was viewed as "a clever crime" (Sandberg, 1995). For instance, in 1995, Kevin D. Mitnick was charged of breaking into corporate computers, stealing thousands of credit card records and software. He was a featured figure in a book and was regarded by his fans as a "legend," a "technology-wielding genius," and a "hero" (Sandberg, 1995). Nowadays, the media mostly portrays a negative image of cybercrimes (Best, 2003; Furnell et al., 1999). Nowadays, cybercrimes' impacts are more clearly identified and understood. An Economist (2007) article notes: "As botnets evolve from simple vandalism to sophisticated criminality, people take them more seriously."

In the cyberworld, we expect that an increase in the rate of cybercrimes leads to an increase in the reporting of such crimes. It is also reasonable to expect that over time stigma associated with becoming a cybercrime victim will decrease and reporting of such a crime may increase. Gill and Gropp (1997) quote a computer-security expert: "there used to be an unspoken stigma about computer crime. For a company to prosecute computer theft was to publicly announce its vulnerabilities and invite copycats." Liebermann (2008) noted: "As companies report a greater number of these breaches, the perceived stigma of such a breach will lessen. Once companies accept that—just like all banks report armed robbery—all companies should report cyber breaches, investigations of such breaches will begin earlier and have greater success."

5.5.2.1 Glamour Associated with the "Hacker" Label

An issue that deserves mention relates to the glamour associated with the "hacker" label. As noted above, as late as the 1980s, "hackers" were considered to be people with high level of computing skills. Following Garvin's (1987) "unstated analogy," we can argue that individuals perceive the image of hacking activities "today" as similar to the image "yesterday." This institutional inertia effect has increased the attractiveness of hacking activities in general.

Many teens are still attracted by the glamour surrounding the "hacker" label. A major problem is related to youths' inability to distinguish the boundary between white hat hacking and criminal hacking (Rao, Monin, & Durand, 2005). Organized crime groups have recruited young people in cybercrime enterprises (BBC news, 2006). According to a March 2007 *McAfee Virtual Criminology Report* produced with the United States and European high-tech crime units, 88% of computer science students at a US university admitted committing an illegal act online. David Marcus, security research and communications manager with McAfee observed: "They watch for bright kids and they start them on small tasks, like 'Find me 100 passwords and I'll give you 1,000 rubles' " (Sullivan, 2007). Another McAfee analyst noted that Crime gangs are recruiting and training teenagers as young as 14 for cybercrimes (Personal Computer World, 2007).

A final issue that deserves mention relates to potential social benefit associated with white hat hacking. It is argued that hacking may also generate social benefit by exposing security flaws (Best, 2003). Most obviously, these types of hacking activities tend to be honored rather than being stigmatized. To take one example, 'Back Orifice' released by the hacker group Cult of the Dead Cow (cDc) was intended to exploit vulnerabilities in Microsoft's Windows 95 and 98 (Best, 2003). Similarly, L0pht created L0phtCrack, which illustrated a flaw in Windows NT (Thomas, 2002).

5.5.2.2 The Hollywood Effect

Many youths adopt their role models from Hollywood (Welsch, 1998).[5] Many hackers have found their role models in cyberpunk sci-fi stories and especially, Hollywood movies have helped shape the cultural image of hacking (Brandt, 2001). The 1982 movie, *Tron*, portrayed "triumph of individual (hacker) good over corporate evil" (Brandt, 2001). Speaking of *WarGames*, Christopher Null (2003) notes: "[the movie] sparked an almost inconceivable interest in computer hacking among our juvenile intelligencia (I was one of them), and the movie's effect on Hollywood and the American consciousness can still be seen today." Likewise, the theme of *Real Genius* (1985) was that hackers are young geniuses, who understand and respect technology better than the adults who create it (Brandt, 2001).

Beginning the 1990s, however, digital crimes increased rapidly. Accordingly, in the latter half of the 1990s, there were several widely publicized movies, in which hacker engaged in criminal activities. Hackers were no longer a harmless character (Brandt, 2001). The *Hackers* (1995) was the first movie to focus solely on the hacker community. The film portrayed hacker as a "quintessentially teenage miscreant" (Levi, 2001, pp. 46–47). In the movie, teenage hackers are engaged in criminal hacking activities, who, in an attempt to extort money, threaten to release a destructive virus (Brandt, 2001). Likewise, in *Goldeneye* (1995), a hacker in Siberia helps the villains steal a high-tech helicopter and a satellite weapon, with capability to disrupt networks located in hundreds of miles away (Brandt, 2001).

Based on above discussion, we can thus argue that anti-cybercrime societal norms are stronger in a society with a higher concentration of cybercrimes than in one with a lower concentration of cybercrimes.

5.5.3 The Formation of Cognitive Pillar Around Cybercrime

Cognitive institutions are associated with culture (Jepperson, 1991). In most cases, they are based on subconsciously accepted rules and customs as well as some taken-for-granted cultural account of cybercrime-related activities (Berger & Luckmann, 1967). Anti-cybercrime cognitive institutions are also associated with consumers' cultural resources related to behaviors, dispositions, knowledge, and habits internalized through socialization (Bourdieu, 1986).

The real question is how anti-cybercrime habits and practices develop among organizations and Internet users. Note that anti-cybercrime practices include staying away from cybercrime as well as helping to combat cybercrimes. As noted earlier, most people using computer networks unethically do not perceive ethical implications of their actions (Kallman & Grillo, 1996). Consider, for instance, piracy, a form of cybercrime. It should be noted that software sharing was more common in the United States when computers were rare and found mostly in universities (Gallaway & Kinnear, 2004). There is some evidence that parents, and even teachers, advocate certain computer crimes, particularly software piracy among students (Bowker, 2000). The Chronicle of Higher Education (2007) noted: "We continue to seek technological, legislative, and law-enforcement solutions to what is largely an educational problem." For some cybercrime victims, it also takes some time to realize that they have been victims (Wall, 1998; Richtel, 1999).

Different theoretical contributions and various empirical studies have led to the accepted view that when institutional rules and norms are broadly diffused and supported, organizations are more likely to acquiesce to these pressures because their social validity is less likely to be questioned (Knoke, 1982; Oliver, 1991; Tolbert & Zucker, 1983). For instance, Knoke (1982) found that one of the best predictors of a municipality's adoption of reforms was the proportion of other municipalities that had adopted such reforms. Likewise, Tolbert and Zucker's (1983) study indicated that the degree of diffusion of civil service policies and programs was positively related to the probability of adoption by a firm that had not yet adopted such policies and programs. We extend this logic to argue that increased Internet penetration and consumers' and businesses' longer experiences facilitate the development of habits and practices consistent with an anti-cybercrime logic. To take one example, in 2005, Priceline.com started working on a draft of the company's adware policy (Heun, 2005). Likewise, more experienced users are likely to be more capable to realize that they are victimized.

5.5.3.1 The Novelty Factor

A US attorney argued that a cybercrime is "a clever crime" and "everyone's impressed" (Sandberg, 1995). The 1995 arrest of Kevin D. Mitnick, who was charged of cracking dozens of corporate computers, stealing thousands of credit card records and software, provides a remarkable example of how the society perceives such crimes. The public handled it as a "heroic act" or "a funny story" (Zombori, 2001). He was a featured figure in a book and was regarded by his fans as a "legend," a "technology-wielding genius" and a "hero" (Sandberg, 1995; New York Times, 1995). More broadly, American society has been very fond of clever outlaws (Sandberg, 1995).

Reflective pieces from the popular press and academic articles have illustrated how different forms of cybercrimes lack stigma. It is, for instance, argued that there is no public and social stigma if an operator of an online gambling is caught. Clark (1998) observes: "in fact the opposite is often the case." Likewise some analysts observe that "Internet gambling [lacks] ... the social stigma of gambling" (The Washington Post, 1998). Other similar examples have been noted in Chap. 2. The real issue thus concerns a lack of social stigma in cybercrimes.

5.6 Concluding Comments

In this chapter, we examined the nature institutional legitimacy for cyber-criminals. This matters not only for theoretical reasons, but also for practical ones. Hacking and cybercrime are going through a rapid transition phase. In the past two decade, most industrialized countries have enacted many laws to deal with cybercrimes and have developed other regulatory infrastructures. Yet, notwithstanding the accomplishments on the regulative front, normative and cognitive institutions related to cybercrime have been relatively slow to change. Informal institutions inherited from the past have helped the growth of this industry. For instance, traditionally cybercrime victims were stigmatized and cyber-criminals were honored. A related point is that while hackers share the things they find, attack victims are embarrassed to publicize their vulnerabilities and fear that it would aid other attackers (Paller, 1998).

They thus tend to hide such information. There is, however, some indication that this situation is changing.

Regulators in industrialized countries have a plenty of wind in their sails. Due to institutional inertia, the seriousness of cybercrimes and their far-reaching influence seem to be underrecognized in the political community. Well coordinated, well funded campaigns are thus needed to combat cybercrimes. By well coordinated, we mean a better international, inter-governmental agency, and government–business collaborations and coordination to fight cybercrimes. It is also necessary to increases resources and funding to fight cybercrimes in proportion to the impact of such crimes.

The novelty effect of hacking is expected to decline with a higher level of cybercrime in a society and the public's longer experience with the Internet (Coates & Humphreys, 2008). Likewise, anti-cybercrime codes, policies, principles, standards, and procedures are likely to develop over time. The example of piracy helps explain the processes that underlie the gradual development of anti-cybercrime cognitive institutions. It should be noted that software sharing was more common in the United States when computers were rare and found mostly in universities (Gallaway & Kinnear, 2004). Nowadays, public awareness toward intellectual property protection has increased. In sum, anti-cybercrime normative and cognitive institutions are likely to be stronger in a society that has more experienced consumers and businesses than in one with less experienced consumers and businesses.

We discussed various examples of exogenous shocks. Some analysts, however, believe that these external shocks have not been big enough to lead to the development of strong anti-cybercrime institutions. In 2003, Mike McConnell, a former director of the US National Security Agency, noted that until "there is a cyber 9/11," or "without something that serves as a forcing issue," governments and the private sector would not be prepared for attack (Cant, 2003).

Finally, in some developing economies, efforts to develop regulative institutions have been mainly directed toward protecting the ruling regimes' interests instead of ensuring the security of the country and its citizens. In Pakistan, for instance, the Interior Ministry announced in July 2009 that acts such as mocking the president via text messages, e-mail, or blogs may face prison sentences of up to 14 years under a new Cybercrimes Act (Ahmed, 2009). Likewise, in China, about 30,000–40,000 cyber police "patrol" the Internet including chat rooms and Weblogs, who also provide viewpoints that are favorable to the Communist Party of China (CPC) (Cannici, 2009; Kshetri, 2008).

Notes

1. It is important to note that most cybercrimes are associated with hacking.
2. Hannigan (1995, p. 64) identified three types of disruptive events: milestones; catastrophes; and legal/administrative happenings.
3. Resources are tangible (economic/financial, human) and intangible (cultural, social, symbolic) (Misangyi et al., 2008). We, however, deal with only tangible resources in this chapter.

4. The CAN-SPAM Act is a law that "sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have . . . stop emailing them, and spells out tough penalties for violations" (ftc.gov, 2009).
5. Welsch (1998) observes: "One gangster compares himself to Jesse James and Al Capone by turns; another comments that he likes it when the movies make the mob boss 'good looking' ".

References

Ahmed, I. (2009). Zardari's popularity sags – Will it undermine Pakistan's fight with Taliban? *Christian Science Monitor*. http://www.csmonitor.com/2009/0909/p06s01-wosc.html. Accessed 30 October 2009.

Amenta, E. (1998). *Bold relief*. Princeton, NJ: Princeton University Press.

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

Asner, M. A., & Kleyna, M. (2009). The new white house cyber czar. *Computer & Internet Lawyer, 26*(7), 1–4.

Balganesh, S. (2008). Demystifying the right to exclude: Of property, inviolability, and automatic injunctions. *Harvard Journal of Law and Public Policy, 31*(2), 593–661.

Bank, D. (2005, February 24). Companies seek to hold software makers liable for flaws. *Wall Street Journal,* B.1.

Barnett, W. P., & Carroll, G. R. (1993). How institutional constraints affected the organization of early US telephonies. *Journal of Law, Economics and Organization, 9*, 98–126.

Bartley, T. (2007). How foundations shape social movements: The construction of an organizational field and the rise of forest certification. *Social Problems, 54*(3), 229–256.

BBC News. (2006, December 8). Criminals 'target tech students'. http://news.bbc.co.uk/2/hi/technology/6220416.stm. Accessed 1 September 2009.

Bell, N., & Tetlock, P. E. (1989). The intuitive politician and the assignment of blame in organizations. In R. A. Giacalone & P. Rosenfeld (Eds.), *Impression management in the organization* (pp. 105–124). Hillsdale, NJ: Lawrence Erlbaum Associates.

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

Best, K. (2003). The Hacker's challenge: Active access to information, visceral democracy and discursive practice. *Social Semiotics, 13*(3), 263–282.

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.

Bourdieu, P. (1986). The forms of capital. In J. Richardson (Ed.), *Handbook of theory and research for the sociology of education* (pp. 241–258). London: Greenwood Press.

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

Brandt, A. (2001). Hacking Hollywood. http://pcworld.about.com/news/Apr042001id45804.htm. Accessed 1 September 2005.

Cannici, Jr., W. J. (2009). The global online freedom act: combating american businesses that facilitate internet censorship in China. *Journal of Internet Law, 12*(11), 3–17.

Cant, S. (2003, April 22). 'Cyber 9/11' risk warning. *The Sydney Morning Herald*. http://www.smh.com.au/articles/2003/04/21/1050777200225.html. Accessed 1 September 2009.

Claburn, T. (2009, October 30). Facebook wins $711 million from spammer. *Information Week*. http://www.informationweek.com/news/global-cio/security/showArticle.jhtml?articleID=221400140. Accessed 31 October 2009.

Clark, B. (1998). *Techno gambling: Stepping outside the cyber-gambling square*. Paper presented at the conference Gambling, Technology and Society: Regulatory Challenges for the 21st Century, convened by the Australian Institute of Criminology in conjunction with the Australian Institute for Gambling Research, Sydney.

Clemens, E., & Cook, J. (1999). Politics and institutionalism: Explaining durability and change. *Annual Review of Sociology, 25*, 441–466.

Coates, D., & Humphreys, B. R. (2008). Novelty effects of new facilities on attendance at professional sporting events. *Contemporary Economic Policy, 23*(3), 436–455.

Computer Fraud & Security. (2002). News: Should software vendors be responsible for security vulnerabilities? 2002(2), 4–5.

Covaleski, M., & Dirsmith, M. (1988). An institutional perspective on the rise, social transformation, and fall of a university budget category. *Administrative Science Quarterly, 33*, 562–587.

Cuéllar, M. (2004). The mismatch between state power and state capacity in transnational law enforcement. *Berkeley Journal of International Law, 22*(1), 15–58.

Daokui Li, D., Feng, J., & Jiang, H. (2006). Institutional entrepreneurs. *American Economic Review, 96*(2), 358–362.

Davis, J. B. (2006). Cybercrime fighters. *ABA Journal, 89*, 36.

DiMaggio, P. J. (1988). Interest and agency in institutional theory. In L. G. Zucker (Ed.), *Institutional patterns and organizations: Culture and environment*, (pp. 3–22). Cambridge, MA: Ballinger.

DiMaggio, P. (1991). Constructing an organizational field as a professional project: U.S. art museums, 1920–1940. In W. W. Powell & P. J. DiMaggio (Eds.), *The new institutionalism in organizational analysis* (pp. 267–292). Chicago: University of Chicago Press.

Economist.com. (2007, August 30). Global Agenda. A walk on the dark side. *Europeview*, 1.

Evans, J. (2000). Cyber-crime laws emerge, but slowly. http://archives.cnn.com/2000/TECH/computing/07/05/cyber.laws.idg. Accessed 1 September 2005.

Fligstein, N. (1991). The structural transformation of American industry: An institutional account of the causes of diversification in the largest firms: 1919–1979. In W. Powell & P. DiMaggio (Eds.), *The new institutionalism in organizational analysis* (pp. 311–336). Chicago: University of Chicago Press.

Friedland, R., & Alford, R. R. (1991). Bringing society back in: Symbols, practices, and institutional contradictions. In W. W. Powell & P. J. DiMaggio (Eds.), *The new institutionalism in organizational analysis* (pp. 232–263). Chicago: University of Chicago Press.

ftc.gov. (2009, September). Facts for business. http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm. Accessed 31 October 2009.

Furnell, S. M., Dowland, P. S., & Sanders, P. W. (1999). Dissecting the “Hacker Manifesto”. *Information Management & Computer Security, 7*(2), 69–75.

Gallaway, T., & Kinnear, D. (2004). Open source software, the wrongs of copyright, and the rise of technology. *Journal of Economic Issues, 38*(2), 467–474.

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

Garvin, D. A. (1987). Competing on the eight dimensions of quality. *Harvard Business Review, 65*, 101–109.

ghanabusinessnews.com. (2009). Church prays against cyber crime in Ghana. http://ghanabusinessnews.com/2009/06/01/church-prays-against-cyber-crime-in-ghana. Accessed 1 September 2009.

Gill, M. S., & Gropp, G. (1997). Cybercops take a byte out of computer crime. *Smithsonian, 28*(2), 114–124.

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

Greenemeier, L. (2006). New from cybercrooks: Fake chrome, pump-and-dump. *InformationWeek, 1112*, 26.

Greenwood, R., & Hinings, C. R. (1996). Understanding radical organizational change: Bringing together the old and the new institutionalism. *Academy of Management Review, 21*, 1022–1054.

Greenwood, R., Suddaby, R., & Hinings, C. R. (2002). Theorizing change: The role of professional associations in the transformation of institutionalized fields. *Academy of Management Journal, 45*(1), 58–80.

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.

Hannigan, J. (1995). *Environmental sociology*. New York: Routledge.

Hardy, C., & Phillips, N. (1998). Strategies of engagement: Lessons from the critical examination of collaboration and conflict in an organizational domain. *Organization Science, 9*(2), 217–230.

Hart, H. L. A. (1961). *The concept of law*. Oxford: Clarendon Press.

Haveman, H. A., & Rao, H. (1997). Structuring a theory of moral sentiments. *American Journal of Sociology, 102*, 1606–1651.

Haveman, H. A., Russo, M. V., & Meyer, A. D. (2001). Organizational environments in flux: The impact of regulatory punctuations on organizational domains, CEO succession, and performance. *Organization Science, 12*, 253–273.

Heun, C. T. (2005). Can spyware ever come in from the cold? *InformationWeek, 1061*, 70–71.

Hicks, A. (1999). *Social democracy and welfare capitalism*. Ithaca: Cornell University Press.

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

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

Huber, E., & Stephens, J. D. (2001). *Development and crisis of the welfare state*. Chicago: University of Chicago Press.

Identity and Access Management (IAM). (2007). Software Quality: The UK Report on Internet Security. http://community.ca.com/blogs/iam/archive/2007/08/14/software-quality-the-uk-report-on-internet-security.aspx. Accessed 1 September 2008.

Jenkins, J. C., Leicht, K. T., & Wendt, H. (2006). Class Forces, Political Institutions, and State Intervention: Subnational Economic Development Policy in the United States, 1971–1990. *The American Journal of Sociology, 111*(4), 1122–1182.

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

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

Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist, 58*, 697–720.

Kallman, E. A., & Grillo, J. P. (1996). *Ethical decision making and information technology*, 2e. New York: McGraw Hill.

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

Knoke, D. (1982). The spread of municipal reform: Temporal, spatial, and social dynamics. *American Journal of Sociology, 87*(6), 1314–1339.

Korosec, R. L., & Berman, E. M. (2006). Municipal support for social entrepreneurship. *Public Administration Review, 66*(3), 448–462.

Kshetri, N. (2004). Economics of linux adoption in developing countries. *IEEE Software, 21*(1), 74–81.

Kshetri, N. (2008). *The rapidly transforming Chinese high technology industry and market: Institutions, ingredients, mechanisms and modus Operandi*, Caas Business School, City of London and Chandos Publishing (Oxford).

Kshetri, N., & Dholakia, N. (2001, August). *Impact of cultural and political factors on the adoption of digital signatures in Asia*. Proceedings of the Americas' conference on Information System (AMCIS), Boston.

Larkin, M. (2000). Websites in brief. *The Lancet, 355*(9216), 1735.

Leblebici, H., Salancik, G. R., Copay, A., & King, T. (1991). Institutional change and the transformation of interorganizational fields: An organizational history of the US radio broadcasting industry. *Administrative Science Quarterly, 36*, 333–363.

Levi, P. (2001). Between the risk and the reality falls the shadow: Evidence and urban legends in computer fraud. In D. Wall (Ed.), *Crime and the internet.* London, England: Routledge.

Liebermann, E. (2008). A collective crackdown on cybercrime. http://www.internetevolution.com/author.asp?section_id=490&doc_id=144804&. Accessed 1 September 2009.

Lorange, P., Scott, M. M., & Ghoshal, S. (1986). *Strategic control systems*. St. Paul: West.

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

Maguire, S., Hardy, C., & Lawrence, T. B. (2004). Institutional entrepreneurship in emerging fields: HIV/AIDS treatment advocacy in Canada. *Academy of Management Journal, 47*(5), 657–679.

Massey, J. A. (2006). The emperor is far away: China's enforcement of intellectual property rights protection, 1986–2006, *Chicago Journal of International Law, 7*(1), 231–237.

Mead, N. R. (2004). Who is liable for insecure systems? *Computer, 37*(7), 27–34.

Meyer, A. D., Brooks, G. R., & Goes, J. B. (1990). Environmental jolts and industry revolutions: Organizational responses to discontinuous change. *Strategic Management Journal, 11*, 93–110.

Meyer, A. (1982). Adapting to environmental jolts. *Administrative Science Quarterly, 27*, 515–537.

Meyer, A. D., Gaba, V., & Colwell, K. A. (2005). Organizing far from equilibrium: Nonlinear change in organizational fields. *Organization Science, 16*, 456–473.

Miller, H. (2002). Penalizing vendors brings consequences. *Network World*. http://www.networkworld.com/columnists/2002/0422faceoffno.html. Accessed 1 September 2003.

Misangyi, V. F., Weaver, G. R., & Elms, H. (2008). Ending corruption: The interplay among institutional logics, resources, and institutional entrepreneurs. *Academy of Management Review, 33*(3), 750–770.

Moore, M. (2009, September 4). 50 things that are being killed by the internet. *Telegraph.co.uk.* http://www.telegraph.co.uk/technology/6133903/50-things-that-are-being-killed-by-the-internet.html. Accessed 27 October 2009.

Morning Edition. (2000). Profile: Government claims that they lack appropriate resources to fight cybercrime. *Morning Edition*, 1.

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.

New York Times. (1995, July 2). Hacker is said to agree to a plea bargain, p. I22, http://www.nytimes.com/1995/07/02/us/hacker-is-said-to-agree-to-a-plea-bargain.html. Accessed 31 October 2009.

New York Times. (2000, March 14). New federal web site seeks to counter hackers, A19. http://www.nytimes.com/2000/03/14/us/national-news-briefs-new-federal-web-site-seeks-to-counter-hackers.html. Accessed 31 October 2009.

Null, C. (2003). WarGames, film review by Christopher Null – 2003 Filmcritic.com. http://www.toptenreviews.com/scripts/eframe/url.htm?u=http://www.filmcritic.com/misc/emporium.nsf/ddb5490109a79f598625623d0015f1e4/137bf7e25ae567f188256de900147c08?Open Document. Accessed 1 September 2004.

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of Management Review, 16*, 145–179.

Paller, A. (1998). CyberCrime come to Washington. *Government Executive, 30*(9), 59–63.

Personal Computer World. (2007). Criminals Recruiting Students for Cyber-Crime.

Phillips, N., & Brown, J. (1993). Analyzing communication in and around organizations: A critical hermeneutic approach. *The Academy of Management Journal, 36*(6), 1547–1576.

Phillips, N., Lawrence, T. B., & Hardy, C. (2000). Inter-organizational collaboration and the dynamics of institutional fields. *Journal of Management Studies, 37*(1), 23–43.

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

Purdy, J. M., & Gray, B. (2009) Conflicting logics, mechanisms of diffusion, and multilevel dynamics in emerging institutional fields. *Academy of Management Journal, 52*(2), 355–380.

Rao, H., Monin, P., & Durand, R. (2003). Institutional change in Toque Ville: Nouvelle Cuisine as an identity movement in French gastronomy. *American Journal of Sociology, 108*(4), 795–843.

Rao, H., Monin, P., & Durand, R. (2005). Border crossing: Bricolage and the erosion of categorical boundaries in French gastronomy. *American Sociological Review, 70*(6), 968–992.

Reay, R., Golden-Biddle, K., & GermAnn, K. (2006). Legitimizing a new role: Small wins and microprocesses of change. *Academy of Management Journal, 49*, 977–998.

Richtel, M. (1999, June 2). Federal cybercrime unit hunts for hackers. *New York Times*, A16.

Rustad, M. L., & Koenig, T. H. (2005). The tort of negligent enablement of cybercrime. *Berkeley Technology Law Journal, 20*(4), 1553–1611.

Ryan, D. J. (2003). Two views on security software liability: Let the legal system decide. *IEEE Security & Privacy*, 70–72.

Saad, L. (2009, October 16). Two in three Americans worry about identity theft. *Gallup*. http://www.gallup.com/poll/123713/Two-in-Three-Americans-Worry-About-Identity-Theft.aspx. Accessed 16 October 2009.

Salu, A. O. (2004). Online crimes and advance fee fraud in nigeria – Are available legal remedies adequate? *Journal of Money Laundering Control, 8*(2), 159–167.

Sandberg, J. (1995, February 27). On-line: Immorality play: Acclaiming hackers as heroes. *Wall Street Journal,* B1.

Schneiberg, M. (2005). Combining new institutionalisms: Explaining institutional change in American property insurance. *Sociological Forum, 20*, 93–137.

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.

Strang, D., & Meyer, J. (1993). Institutional conditions for diffusion. *Theory and Society, 22*, 487–511.

Sullivan, B. (2007, April 10). Who's behind criminal bot networks? http://redtape.msnbc.com/2007/04/whos_behind_cri.html. Accessed 1 September 2008.

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.

Tetlock, P. E. (2002). Social functionalist frameworks for judgment and choice: Intuitive politicians, theologians and prosecutors. *Psychological Review, 109*, 451–471.

The Chronicle of Higher Education. (2007, January 5). We must educate young people about cybercrime before they start college. *53*(18), B.29.

The Washington Post. (1998, August 17). Internet gambling: A bad bet, A.18.

Thomas, D. (2002). *Hacker culture*. Minneapolis, MN: University of Minnesota Press.

Thornton, P. H., & Ocasio, W. (1999). Institutional logics and the historical contingency of power in organizations: Executive succession in the higher education publishing industry, 1958–1990. *American Journal of Sociology, 105*, 801–843.

Tolbert, P. S., & Zucker, L. G. (1983). Institutional Sources of Change in the Formal Structure of Organizations: The Diffusion of Civil Service Reform, 1880–1935. *Administrative Science Quarterly, 28*, 22–39.

USA Today. (2002). Microsoft Glitches Prompt Liability Concerns. http://www.usatoday.com/tech/news/2002/06/17/microsoft-security.htm.

Wall, D. S. (1998). Catching cybercriminals: Policing the internet. *International Review of Law, 12*(2), 201–218.

Welsch, T. (1998). Killing them with tap shoes: Violent performance in The Cotton Club. *Journal of Popular Film & Television, 25*(4), 162–171.

White, H. (1992). *Identity and control: A structural theory of social interaction*. Princeton, NJ: Princeton University Press.

Wiesenfeld, B. M., Wurthmann, K. A., & Hambrick, D. C. (2008). The stigmatization and devaluation of elites associated with corporate failures: A process model. *Academy of Management Review, 33*(1), 231–251.

Wong, L., & Tang, J. (2006/2007). Dilemmas confronting social entrepreneurs: Care homes for elderly people in Chinese cities. *Pac Aff, 79*(4), 623–640.

Zombori, G. (2001). *e + Finance + Crime: A Report on Cyber-Crime and Money Laundering*, Study of Organized Crime and Corruption, Osgoode Hall Law School, York University, Toronto, Ontario, Canada, 5 January. http://www.yorku.ca/nathanson/Publications/e.htm.