Chapter 6
Information and Communications Technologies, Cyberattacks, and Strategic Asymmetry

Criminals, for their part, are motivated by greed. Few leaders of the cyber-organized crime world would hesitate to sell their capabilities to a terrorist loaded with hard currency. That, combined with the ever-growing terrorist awareness of cyber vulnerabilities, makes this set of scenarios not just highly likely, but close to inevitable (Bucci & Steven, 2009).

"If you're able to take down part of the electrical grid, pretty much everything else fails . . .. You're not back in the 1970s; you're back in the 1870s." James Woolsey, former director of the US Central Intelligence Agency (cf. Maltz, 2009).

Abstract In the history of warfare, there are a number of examples of strategic uses of asymmetric technologies. Consistent with history and theory, individuals, organizations, and nations have spotted opportunities to employ information and communications technologies to gain and exploit asymmetric advantages and to counter asymmetric weaknesses. This chapter discusses various asymmetries associated with institutions, nations, and organizations that influence the ICT-security nexus. Regulative, normative, and cognitive institutions in a country provide various mechanisms that affect the nature of positive and negative asymmetries. Nations and organizations also differ in terms of their capability to assimilate ICT tools to gain positive asymmetries and deal with vulnerabilities of negative asymmetries.

6.1 Introduction

Information and communications technologies (ICTs) have fundamentally changed the equations related to security functions of nations, organizations, and individuals (e.g., English, 2005; Metz, 2001; Zhou, 2005). The vulnerability to threat as well as the capability to strategically deploy ICTs varies across entities. The characteristics of organizations, nations, and institutions superimpose in a unique interaction with ICTs' nature that influence the ICT-security nexus.

N. Kshetri, *The Global Cybercrime Industry*, DOI 10.1007/978-3-642-11522-6_6,

This chapter explores the nature of ICT-related asymmetries (see Table 6.1 for definitions of terms) from the perspective of national, organizational, and individual security. Asymmetry created by ICTs (more broadly: technologies) is among six forms of asymmetry identified by Metz and Johnson (2001). Nations and organizations can exploit asymmetric advantages by strategically employing ICTs in war against enemies (e.g., cyberattacks) as well as by using ICTs in facilitating other functions contributing to attack and defense such as communications, detection of threats from enemies, gathering intelligence. For instance, it was reported that in

Table 6.1 Explanation of major terms used in the chapter

Term	Explanation
Encryption technologies	These technologies transform text or data into a coded form that is close to impossible to read without the key to decode the message. This scrambling of the message is done by using a mathematical formula
ICTs[a]	These include telecommunications as well as digital technologies such as telephony, cable, satellite, radio, computers, information networks, and software
Negative asymmetry[b]	A difference an adversary is likely to use to exploit a weakness or vulnerability
National security	"Measures taken by a state to ensure its survival and safety". "Includes the deterrence of attack, from within and without, as well as the protection and well-being of citizens"[c]
Positive asymmetry[b]	Capitalizing on differences to gain an advantage.
Steganography[d]	A technique that allows hiding messages within pictures, music, and other media. Steganography can be used with or without encryption. It is, however, of limited use without encryption
Symmetric advantage[b]	The advantage that can result from matching the opponent in terms of strategic resources
Strategic asymmetry[b]	Employing "some sort of differences to gain an advantage over an adversary." It could be real as well as perceived
The Gramm-Leach-Bliley Act[e]	The Gramm-Leach-Bliley Act of 1999 went into effect in July 2002. It mandates that all financial institutions establish procedures for protecting personal information, including the protection of discarded information. Financial penalties and civil suits may result from the inadvertent disclosure of personal information
The USA Patriot Act[f]	The USA Patriot Act was enacted on October 26, 2001 to expand the intelligence gathering and surveillance powers of law-enforcement and national security agencies

[a] See "Glossary of Terms," http://cyber.law.harvard.edu/readinessguide/glossary.html (accessed 16 October 2009).
[b] Metz (2001) and Metz and Johnson (2001).
[c] See http://en.wikipedia.org/wiki/National_security (accessed 16 October 2009).
[d] Maney (2001) and Hernandez, Sierra, and Ribagorda (2004).
[e] http://www.allshredservices.com/faq/grammleachbliley.htm
[f] Young (2004).

the planning phase of the Mumbai attacks in 2008 in India, the attackers were using VoIP for communications (Aggarwal, 2009). The Internet as well as non-Internet ICTs such as wireless telephony, satellite TV, satellite phones, and supercomputers can be employed in the management of asymmetries (see Table 6.2).

In the history of warfare, there are several examples of strategic uses of asymmetric technologies that have provided "a decisive advantage over an opponent in combat" (Rosenberger, 2005). The Maxim Machine-Gun adopted by the British Army in 1889 is a good example of an asymmetric technology. A Maxim gun could fire 500 rounds per minute—equivalent to that of 100 rifles at that time. In the 1893–1894 Matabele war, 50 British soldiers with just four Maxim guns fought off 5,000 Matabele warriors (spartacus UD). Similarly, asymmetric technologies used by the US Army include cruise missiles, laser-guided bombs, satellite reconnaissance systems, high-altitude reconnaissance aircraft, and unmanned aerial vehicles (Rosenberger, 2005).

The example of a strategic disruption of the enemy's communications technology goes back at least to the mid-19th century in the American Civil War. On October 4, 1862, for example, a landing party from Thomas Freeborn, a steamer acquired by the Union Navy, cut the telegraph lines stretching from Occoquan and Fredericksburg to Richmond, Virginia (The Economist, 2008a). Likewise, in the Russo-Japanese War of 1904–1905, the Russian navy used radio jamming to block and frustrate the Japanese Military's communications.

Consistent with history and theory, organizations and nations have spotted opportunities to employ ICTs to gain and exploit asymmetric advantages and to counter asymmetric weaknesses. For instance, in the Iraq War, powerful ICT tools such as *Analyst's Notebook* allowed US investigators to convert huge amount of data into actionable intelligence. The intelligence helped to track the wanted Iraqis. *Analyst's*

Table 6.2 A classification of strategic asymmetry by type of ICTs and type of deployment: Some examples

		Type of deployment	
		Direct use in war	Facilitating functions contributing to attack and defense
Type of ICTs	Internet	• Cyberattacks on critical infrastructures	• Communications (e.g., Al Qaeda's encrypted e-mails; the attackers in the Mumbai attacks in 2008 used VoIP for their planning and communications) • Detection of threats from enemies (smart containers in US customs)
	Non-Internet ICTs	• Use of satellite phones to coordinate war plans (e.g., by Al Qaeda)	• Use of supercomputers to model nuclear explosions and to simulate the forces acting on a missile

Notebook also helped to trace the creator of "love bug" computer virus of 2000 (Yousafzai & Hirsh, 2004). The US military and intelligence officials are using the same technology to track Al Qaeda's network. Al Qaeda's network, on the other hand, has been reportedly using symmetric and asymmetric technologies[1] including satellite phones, the Internet, and advanced encryption methods to recruit followers; raise money; formulate plans and operations; and to communicate securely (see Box 6.1).

Box 6.1 Al Qaeda's Amazingly Advanced Internet Network

Experts believe critical US infrastructures such as energy, transportation, water, and telecomm are highly susceptible to Al Qaeda's cyberattacks. In the early 2004, Dan Verton, a former intelligence officer, told a Senate subcommittee that one of the goals of Al Qaeda is to overthrow the US economy by penetrating the computer networks of major companies. Although no cyberattack has yet been traced to Al Qaeda, this outfit's network use has been amazingly sophisticated.

Family influence played an important role in Osama bin Laden's fascination with modern technologies (Coll, 2008; *The Economist,* 2008b). A July 1999 article published *in Christian Science Monitor* reported that Al Qaeda's Egyptian members helped establish a secure communications network based on the Internet, e-mail, and electronic bulletin boards for its members to exchange information. According to an article published *in San Francisco Chronicle* on October 6, 2001, Al Qaeda has recruited talented software engineers to achieve its Internet ambition. It is reported that Al Qaeda followers are acquiring skills in operating computers, and Internet connections though satellite (Nance, 2008).

Al Qaeda has been among the earliest adopters of encryption technologies, which employ mathematical formulae to scramble data for secure transmission of information on the Internet. According to the former CIA director George Tenet, these technologies have enabled the organization to formulate plans, strategies, and operations; to recruit followers; spread the network; and to raise fund.

US officials have reported that Bin Laden followers got encryption trainings at camps in Afghanistan and Sudan. A convicted conceiver of the 1993 World Trade Center bombing, for instance, used encryption software to hide the details of his plans to destroy 11 US airliners. Similarly, a suspect in the bombings of US embassies in Kenya and Tanzania in 1998 reportedly sent encrypted e-mails to several recipients. Investigators believe that encryption might have played a key role in the September 11, 2001 attack in the United States.

Al Qaeda's integration of encryption with advanced applications such as steganography has been a real challenge to US counterterrorism officials. The use of steganography software file has helped them hide plaintext messages within a wide range of media such as pictures, music, MP3 files, sports chat rooms, and pornographic bulletin boards. Most impressive of all, Al Qaeda has created "self-starting jihad," an Internet-based campaign to inspire and educate its followers (Nance, 2008). Michael (2009, p. 147) observed: "The Internet is an integral part of al-Qaeda's strategy."

6.2 Strategic Asymmetry and ICTs

True examples of strategic asymmetry are arguably very rare. Experts say that strategic asymmetries are created by combining technological, operational, as well as tactical innovations (Meigs, 2003). Metz and Johnson (2001) have identified six forms of asymmetry: method, technology, will, morale, organization, and patience.

From a terrorist organization's standpoint, cyber-terrorism has some advantages over physical methods. First, cyber-terrorism can be conducted remotely and anonymously. Unlike in the traditional warfare, it is almost impossible to identify the attacker in the IT warfare. Second, cyber-terrorism is cheaper to carry out as it does not require the handling of explosives or a suicide mission. Finally, due to the novelty, journalists and the public are likely to be fascinated by computer attacks. Cyber-terrorism may thus perform better in attracting media coverage than conventional warfare (Denning, p. 281).

At the same time, compared to physical warfare, cyber-terrorism is less effective in some aspects. Note that terrorists want to maximize damages (Harvard Law Review, 2006). Complexity of networks and systems means that it may be harder to control cyberattacks once they are launched. It is also hard to achieve the level of damage that is desired. Since there is no injury, death, or physical harm, cyber-terrorism do not create strong emotional appeal and drama (Denning, 2003, p. 282). Finally, as long as terrorists see their existing techniques are working, they may be unwilling to try new methods such as cyberattacks (Hoo, Goodman, & Greenberg, 1997).

To maximize positive asymmetries and to minimize vulnerabilities of negative asymmetries, the category of asymmetric strategic means should be such that the adversary cannot effectively counter. This is especially important for asymmetries that are deliberately created than those that arise by default.

At this point, it must be emphasized that only "desperate antagonists" depend solely on ICT-created or other types of asymmetric methods (Metz, 2001). Military theorists and empiricists have presented evidence which indicates that integrated approaches that appropriately combine symmetric and asymmetric methods are

more likely to give intended results and to defeat adversaries (Metz, 2001). In particular, given the limitations of ICTs, approaches that combine non-ICT and ICT tools are more effective. For this reason, defense analysts argue that large and powerful nations such as China and Russia pose the most severe threats to the United States because of their technology advanced research (Bridis, 2001) as well as capabilities to combine ICTs with non-ICT resources. It is argued that a cyberattack coordinated with physical attacks could compound the fallout by "disrupting communications, distracting the government response, and exacerbating the psychological damage from terrorism" (Harvard Law Review, 2006).

Before proceeding further, it is important to understand the concepts of positive and negative asymmetries associated with ICTs. ICT deployments by terrorist groups, nations, and individuals involve some forms of positive and negative asymmetries. Positive asymmetry entails capitalizing on differences to gain an advantage.[1] For instance, the US military combines training and leadership (non-ICT resources) with ICTs to gain and sustain its superiority (Metz, 2001). In the war in Afghanistan, special operations forces downloaded real-time video of Al Qaeda and Taliban forces, used GPS to mark the exact locations, and employed LASERS to bring smart bombs directly onto their positions.

Similarly, according to the US-China Economic and Security Review Commission report, Chinese military strategists have written openly about exploiting the vulnerabilities associated with the US military's reliance on ICTs and traditional infrastructure used to conduct operations (GAO Reports June 22, 2007). According to Al Santoli, editor of the *China Reform Monitor*, senior colonels of the Chinese military Qiao Liang and Wang Xiangsui (1999) in their book, *Unrestricted Warfare*, have argued that since China's People's Liberation Army (PLA) lacks resources to compete with the United States in conventional weapons, it should focus on the "development of new information and cyber war technologies and viruses to neutralize or erode an enemy's political, economic and military information and command and control infrastructures" (cf. Waller, 2000). The authors have urged on the development of a means of challenging the United States through asymmetry rather than matching the United States in terms of all types of resources (Waller, 2000). Some analysts suspect that the Chinese government has been using cyberattacks to break into the US Defense Department's and other US agencies' computers, which is code-named Titan Rain by federal investigators (Jesdanun, 2008). Speaking of cyberattacks originated from China and its growing cyberwarfare capabilities, David Sedney, US deputy assistant secretary of defense for East Asia noted: "the techniques that are used, the way these intrusions are conducted, are certainly very consistent with what you would need if you were going to actually carry out cyberwarfare, and the kinds of activities that are carried out are consistent with a lot of writings we see from Chinese military and Chinese military theorists" (World Tribune, 2008).

The United States considers cyberwarfare as one of the major asymmetric threats (Blank, 2004). Estimate suggested that 100–120 countries in the world are planning infowar capabilities and developing cyberattack strategies (Swartz, 2007;

Robertson, 2007). In response, US Defense Secretary Robert Gates initiated the creation of a new military cyber-command, which defends the Pentagon's networks and conducts cyberwarfare (Harris, 2009).

The US National Security Agency and some US observers believe that countries like China, Iran, Russia, and North Korea have developed computer attack capabilities, trained hackers in Internet warfare, and are systematically probing the computer networks in the United States to find weaknesses that can be exploited (Bickers, 2001; Lenzner & Vardi, 2004). Although most are currently only testing cyberattack tools to determine the risks involved, experts argue that serious international cyberattacks may occur in the future (Robertson, 2007). Some analysts observe that cyberattacks on the United States by China have been "frequent and aggressive" (Reid, 2007). It is suggested that there may be over 60,000 cyber-war fighters in China's PLA (Bronk, 2009). Likewise, it is estimated that North Korea has a cyber-military unit, which employs about 1,000 skilled hackers (Sudworth, 2009). The US Central Intelligence Agency has also identified two terrorist organizations that possess the capability and have the greatest possibility to use cyberattacks against the US infrastructures (GAO Reports June 22, 2007).

Not only nations and terrorists but also individuals are employing modern ICTs strategically to gain asymmetric advantages. In 2003, a Pakistani medical transcriber working for a US-based medical centre threatened to post confidential voice files and patient records on the Internet if her pay was not increased. In this example, the transcriber took advantages of the differences in normative institutions (e.g., the medical center's obligation to maintain patients' privacy in the United States) and regulative institutions (e.g., a potential threat of lawsuit for failing to protect patients' information).

Negative asymmetry involves "an opponent's threat to one's vulnerabilities" (Metz, 2001). It is important to note that vulnerability has two dimensions: objective and subjective (Busetta & Milito, 2009; Zombori, 2001). The objective vulnerability is related to political, social, economic, and demographic characteristics of an entity that determine the vulnerability to cyberattacks. The subjective vulnerability refers to an entity's self-perception related to the risk of becoming a cyberattack victim. It is also important to note that an individual's or an organization's vulnerability is determined by the personal or organizational characteristics as well as the contexts provided by "higher" level institutions and exogenous parameters (Busetta & Milito, 2009; Snidal, 1994, 1996).

Organizations and nations are employing ICTs strategically to minimize vulnerabilities associated with negative asymmetry. For instance, Al Qaeda reportedly uses powerful encryption technologies to support its operations. According to a *USA Today* article (Maney, 2001), Al Qaeda is also using more advanced and sophisticated technologies such as steganography to hide messages within pictures, music, and other media. A plaintext message with or without encryption is hidden in a picture or MP3 file using a steganography software file. These technologies have helped Al Qaeda members to communicate without a major risk of being caught by US counterterrorism organizations. Similarly, a suspect in the bombings of the

US embassies in Kenya and Tanzania in 1998 reportedly sent encrypted e-mails under various names (Kelley, 2001). Likewise, a convicted mastermind of the World Trade Center bombing in 1993 used encryption software to hide details of his plan to destroy 11 US airliners. To take yet another example of ICTs' use to minimize vulnerabilities associated with negative asymmetry, consider the Israeli Defense Force's attack into Gaza in the early 2009. Israeli networks experienced a massive distributed DoS attacks (Bucci & Steven, 2009).

6.3 Institutional and Organizational Factors Linked with Positive and Negative Asymmetries

Table 6.3 summarizes how institutional and organizational factors may be linked with positive and negative asymmetries associated with ICTs. The relationships are expressed in terms of dependent and independent variables. In the first two relations, potential positive and negative asymmetries created by business models are dependent variables and regulative legitimacy to such models is an independent variable. In the last six relations, positive and negative asymmetries are dependent variables and constructs, which are related to institutional and organizational factors as independent variables. As indicated in Table 6.3 some of the relations are specific to certain deploying units such as a government and a criminal group. Table 6.4 explains these relationships in more details with some examples.

Table 6.3 How institutional and organizational factors linked with positive and negative asymmetries

	Construct	Positive(+)/negative(–) asymmetry created by ICTs	Measures to deal with vulnerability to negative asymmetry
1	Lack of regulative legitimacy to business model (DV)	Government/citizen (–) (IV)	
2	Lack of regulative legitimacy to business model (DV)	A nation's adversary (+) (IV)	
3	Lack of strong rules of law (IV)	Cyber-criminal (+) (DV)	
4	Strength of normative legitimacy (IV)	(+) DV	(+) DV
5	Perception of ICT-related security threats (IV)	Governments (+) (DV)	Governments (+) (DV)
6	Economic development of a nation (IV)	Governments (+) (DV)	(+) (DV)
7	Higher dependence on digital technologies (IV)	(–) (DV)	
8	Anonymity functions (IV)	(+) (DV)	

Note: IV, independent variable; DV, dependent variable.

Table 6.4 Some sources of ICT-led asymmetries

Source of asymmetry	Explanation	Remarks/examples
Institutions		
Regulatory	• Strength of the rule of laws • Laws to minimize vulnerability to negative asymmetries • Laws directed toward minimizing symmetric advantages of adversaries	• The lack of laws against cyberattacks and the lack of existence of enforcement mechanisms increase positive asymmetries of cyber-criminals • The Patriot act in the United States and China's regulation regarding encryption software • Laws dealing with the export of encryption products (also COCOM restriction)
Normative	• Social obligations • Professional obligations	• ACLU in the US • Honker Union (Red Hackers) of China
Cognitive	• Perception of threat • Perception of adversaries' capability	• China's interpretation of military security associated with ICT import • Chinese military's interpretation of US Army's ability to assimilate ICTs in warfare
Adopting/deploying units		
Capability and rank effect	• Some adopting units are better able to assimilate ICTs than other	• Japan has planned to introduce passports with chips containing biometrics. Developing countries are less capable to take such measures
Vulnerability to attack	• Computer networks of some organizations are more vulnerable to attack	• Financial agencies, online casinos, and e-commerce websites are more likely to be attacked
Compatibility with ICTs	• Some business models are more compatible with ICTs' nature	• Al Quaeda's secure e-mail communications

6.3.1 Institutions, ICTs, and National Security

Institutionalists have recognized that success of an innovation to perform a particular function (e.g., defense and attack) is tightly linked to the context provided by institutions (Storper & Walker, 1989; Sabel & Zeitlin, 1997). Various asymmetries to a unit arise by default because of the nature of the institutions in which the unit is embedded. In particular, institutions in a country influence the equation of national choice in terms of priority and combinations of technologies employed to defend the people and to attack enemies.

In Chap. 3, we discussed Scott's (1995, 2001) three broad categories of institutions—regulative, cognitive, and normative (see Table 6.4). These components influence institutional preference for employing ICTs to create positive and

negative asymmetries. Each set has corresponding legitimacy concerns. Let's take a look at each of the components in turn.

6.3.1.1 Regulative Institutions

First, there are international differences in terms of laws to minimize vulnerability to several forms of negative asymmetries. The US government, for instance, requires commercial banks to secure their networks. The *Patriot Act* and the *Gramm Leach Bliley (GLB) Act* (Table 6.1) require new security measures including customer identification and privacy protection. Notwithstanding the existence of similar regulations for a long time, the *Patriot Act* reflected a change in the banking landscape. These laws are expected to enhance domestic security against terrorism.

To take another example, China's regulation requires companies to reveal the type of encryption software they use for protecting confidential information sent over the Internet, as well as the name, phone number, and e-mail address of every employee using such software. To take yet another example, following September 11, 2001 attacks, the United States has enacted legislations that have resulted in increased electronic surveillance and the ability of Federal agencies to intercept Internet traffic.

Corporations are also facing regulatory pressures to change their business models so as to minimize real and perceived vulnerabilities of negative asymmetry. For instance, Microsoft was forced to open Windows XP, Windows 2000, and other systems programs to government technical security experts of several countries including those of Russia, Britain, the United States, and China.

Second, nations across the world differ in terms of laws directed toward maintaining positive asymmetries. For instance, until the late1990s, the US government did not allow domestic companies to export encryption products with keys of more than 40 bits. Feeling pressure from domestic technology companies, the Clinton Administration, however, allowed exports of 56-bit products and even stronger ones with government permission. Many terrorist groups, nevertheless, can buy encryption software in countries that lack such laws. For instance, encryption devices that Al Qaeda network reportedly uses are commercially available in several countries.

Some laws are directed toward specific sources of threat. In the 1980s, national security concerns from the United States and its allies in the form of a Coordinating Committee for Multilateral Export Security (COCOM), for instance, put restriction on high-technology exports to countries such as China and Soviet Union. Before 1996, China had been denied access to high-performance computers. Despite the disbandment of COCOM in 1994, the US law still restricts the sales of computers that exceed specified performance limits.

Powerful supercomputers can be used to model nuclear explosions and can simulate the forces acting on a missile from launch to impact. These supercomputers thus enable nations to develop nuclear weapons without explosive testing. The United States was concerned that access to powerful supercomputer would allow China, Soviet Union, and their allies to gain and combine symmetric and asymmetric

methods. Before 1996, China experienced a series of failures in its attempt to launch satellites. Following COCOM disbandment, China was able to acquire over 600 high-performance computers from US companies during 1996–1998, with the approval of the Department of Commerce.

Third, nations across the world differ in terms of regulative institutions that help to create positive asymmetry and deal with negative asymmetry. Although criminals in general are emboldened if laws are weak, a much higher degree of jurisdictional arbitrage is available in digital crimes. Many developing economies have no laws prohibiting such crimes. Some nations that have enacted laws against computer crimes, on the other hand, lack enforcement mechanisms.

Likewise, too weak state (Varese, 2002), inefficient police, and weak cybercrime laws (Onlinecasinonews.com, 2004) have provided a fertile ground for Russian Mafia's digital world. In 2000, three alleged members of the Russia-based HangUp Team, which released Berbew and Webber viruses in 2003, were arrested for attacking two local computer networks, but were released with suspended sentences (Grow & Bush, 2005). Experts also argue that law-enforcement officials in countries like 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). Weak rule of laws bolsters the morale of criminals or produces morale asymmetry (Metz & Johnson, 2001).

6.3.1.2 Normative Institutions

Normative institutions are concerned with procedural legitimacy and require individuals and organizations to embrace socially accepted norms and behaviors. National governments and terrorist organizations differ on acceptable norms and behaviors. Pointing out vulnerabilities of unprotected wireless networks in hospitals, for instance, Verton (2003) illustrates how a terrorist sitting in a car in a hospital parking lot can change medical records (e.g., information about blood type) resulting in patients receiving wrong blood types. National governments, on the other hand, are less likely to prescribe such behavior toward civilians.

As we discussed earlier, normative institutions represent obligations and norms in different sections of societies. In some cases, organizations are likely to face several dimensions of obligatory and prescriptive pressures (e.g., from customers, special interest groups, governments, etc.) that are contradictory in nature. For instance, consider the deployment of biometrics technologies. Commercial banks in the United States are experiencing the powerful emotional impact following the incident of September 11, 2001. They do not want to be branded as Al Qaeda's bank (McGeer, 2002). Deployment of biometric technologies can minimize the possibility of banking transactions with terrorists. Investment in biometric thus reduce bank's vulnerabilities associated with negative asymmetry.

At the same time, obligations to protect privacy have hindered the deployment of biometric technologies in these banks. The United States and European countries, for instance, have different views on privacy protection. In the United States,

it is argued that identification systems based on face-recognition technology pose civil liberty threats (Johnson, 2004). The US banks feel more obligated to protect personal privacy of their patrons than their European counterparts. For this reason, US banks are slower to adopt biometric products in a range of services. Most European Union (EU) nations, on the other hand, have included biometric fingerprints in national drivers' licenses.

In 2003, 14 US states had bills related to biometrics, but many of them were not passed because of privacy concerns. As discussed above, non-profit organizations can use social obligation requirements to induce certain behavior. In the US, the lobbying and efforts of organizations like the *American Civil Liberties Union* (ACLU) played key roles in the failure of the bills.[2]

Professional organizations such as the Honker Union of China (or the Red Hackers)[3] also provide normative legitimacy to web attacks. For instance, consider Red Hackers' reaction to accidental bombing of the Embassy of the People's Republic of China in Belgrade, Yugoslavia on May 7, 1999 by a US warplane.

6.3.1.3 Cognitive Institutions

Cognitive institutions are associated with culturally supported habits and exert subtle influences on ICT deployment for proactive security, defense, and protection efforts. Political elites of some nations have realized that they have militarily fallen behind and are employing the Internet to create strategic asymmetry. Russian political and military leaders think that they are losing the cyber-space war to the US during 1991–2001, Moscow circulated among the members of the UN Security Council drafts of a possible arms-control treaty for cyber-space (Adams, 2001).

In addition, Chinese government also suspects that it is under cyberattack from the United States. There has been a deep-rooted perception among Chinese policy makers that Microsoft and the US government spy on Chinese computer users through secret "back doors" in Microsoft products. Computer hardware and software imported from the United States and its allies are subject to detailed inspection. Chinese technicians take control of such goods and either resist or closely monitor if Western experts install them (Adams, 2001). Chinese cryptographers reportedly found an "NSA Key" in Microsoft products, which was interpreted as the National Security Agency. The key allegedly provided the US government back-door access to Microsoft Windows 95, 98, N-T4, and 2000. Although Microsoft denied such allegation and even issued a patch to fix the problem, the Chinese government has not been convinced.

As mentioned earlier, cognitive institutions influence the way people view the reality that surrounds them and the frames through which they make meanings. For instance, consider Chinese military's assessment of US military's capability to assimilate ICTs in warfare. The authors of *Unrestricted Warfare*, for example, have observed that the US Army is too focused on "weapons whose immediate goal is to kill and destroy" and may not be well-equipped in assimilating ICTs in the warfare (Waller, 2000).

6.3.2 Ability to Create Positive Asymmetry and Minimize Vulnerabilities of Negative Asymmetry

Nations and organizations differ in terms of their capability to deploy ICTs to create positive asymmetry and minimize vulnerabilities of negative asymmetry (see Table 6.4).

6.3.2.1 The Rank Effect

ICT deployment for national security tends to diffuse from more advanced to less advanced nations. This is known as the *rank effect* (Gotz, 1999). For instance, currently deployment of anti-fraud technologies is limited to a small elite group of businesses.

The US military officials are seeking to enhance the country's cyberwarfare capabilities. To do so, they are looking beyond defending the Internet and are developing ways to launch virtual attacks on enemies. Lt. Gen. Robert J. Elder Jr., the head of the Air Force's cyberoperations command noted that initial uses are likely to be in "diverting or killing data packets that threaten the nation's systems" (Jesdanun, 2008).

Similarly Japan introduced passports with chips containing biometrics information in 2005 and also is assessing whether to make use of such technology to screen foreign visitors. In the United States, there are a number of automated entry systems to address a wide range of immigration situations, such as vehicular or pedestrian traffic along the Canadian and Mexican borders, or arrivals at international airports (Baron, 1997).

Whereas industrialized countries are rapidly adopting ICTs to create positive asymmetries and to counter asymmetric threats, most developing countries are characterized by lack of resources and inefficient institutions, which hamper the deployment of such measures. Consider, for instance, strategic uses of ICTs in customs organizations to detect and respond to national security threats. To minimize container-oriented terror events, some developed countries have transformed their customs organizations (Lane, 2005). One such example is the deployment of smart containers that use electronic seals, sensors, and GPS systems to record containers' movements. These technologies alert law-enforcement authorities in case of suspicious activities (Gillis & McHugh, 2002, p. 33). The Smart and Secure Tradelanes Pilot Program already employs smart containers using radio frequency identification devices (RFID), GPS, electronic seals, and other Internet-based technologies[4] (McHugh & Damas, 2002). Although some developing economies such as China and Peru are modernizing their customs infrastructure (Lane, 2005), most are far from ready to deploy advanced ICTs in their customs organizations.

Developing countries' lack of resources to enforce laws also hampers their ability to create ICT-related positive asymmetries and deal with negative asymmetries. For instance, according to laws enacted in Pakistan in the early 2000s, Internet cafés were required to check their clients' identity cards (Fisher, 2002) and Internet users

were not allowed to use encryption technology. Nonetheless, these laws had been largely ignored (World IT Report, 2003).

Beyond all that small, less developed countries are less likely to be included in international cybercrime efforts. For instance, as of 2007, to address problems related to international jurisdiction, investigation, and prosecution, the US Department of Justice (DOJ) and the US State Department had agreements with about 40 nations through the G-8 High Tech Crime Working Group (United States Government Accountability Office, 2007). This means that the United States did not have such agreements with about 180 countries by that time.

6.3.2.2 Degree of Dependence on Digital Technologies

Adopting and deploying units also differ in terms of the degree of vulnerability of negative asymmetries. Businesses with a high dependence on digital technologies—such as online casinos, banks, and e-commerce hubs—are the most likely to fall victim to cyberattacks (Kshetri, 2005). A high dependence on digital technologies is a weakness that adversaries can exploit. Garner (1997, p. 1) observed

> Perhaps nowhere is our vulnerability to asymmetric technologies greater than in our relentless pursuit of information superiority. Our vulnerability lies in the realization that the more proficient we become at collecting, processing, displaying and disseminating relevant, accurate information to aid decision makers, the more dependent we become on that capability and therefore the more lucrative a target. (cf. Thomas, 1999)

To some extent, rank effect discussed in the previous section also holds true for vulnerabilities to threat. Cyberattacks, for instance, are more likely to be targeted to developed countries with large networks such as the United States than developing countries. Libicki (2009, p. 70) observed: "The US economy and society are heavily networked; so is its military. The attacker, by contrast, may have no targets of consequence, either because it is not particularly digitized, because its digital assets are not networked to the outside world, or because such assets are not terribly important to its government." Likewise, Dan Verton, the author of *Black Ice: The Invisible Threat of Cyberterrorism* told a Senate subcommittee in the early 2004 that one of the goals of Al Qaeda is "to topple the US economy by breaking encryption algorithms and infiltrating the technological systems of major corporations."

6.3.2.3 Compatibility with ICTs

The experience and business models of some organizations are more compatible (Rogers, 1983, 1995) with modern ICTs and for this reason they are more likely to benefit from digital technology. Because of the anonymity features of modern ICT tools such as the Internet, it is almost impossible to identify the attacker in ICT warfare. The encryption technology has further reinforced the effect. Thanks to ICTs' anonymity, some sources of malicious activities have been able to enjoy a higher degree of positive asymmetry. Victims may not know whether an attacker is a teenager, a terrorist group, a rival company, or a foreign government. For instance, in 2000, a hacker reportedly accessed software blueprints at Microsoft. Detectives

believed the hacker used software from Asia and transferred data to an anonymous e-mail account in Russia (Bridis, 2001). In the Storm Cloud case,[5] US officials were not able to identify with certainty whether the source was a foreign government or a hacking group (Bridis, 2001). To take another example, in the late 2003 and early 2004, the FBI and National Hi-Tech Crime units discovered that computer hackers employed by Russian mafia launched a DOS attack on Worldpay[6] System that affected thousands of online casinos.

The online anonymous communication environment has also provided terrorists with opportunities to escape from laws, social obligations, and taboos; and express whatever they want. In this way, terrorists are using the Internet to tell their "story" directly to the public thus bypassing traditional media. To take an example, Al Qaeda transmitted videos of *Wall Street Journal* reporter Daniel Pearl's execution on the Internet (Hirsh, 2002).

There have also been instances of the uses of encryption software for controversial and illegal purposes. In 1996, a European Commission Communication identified some areas of risk in using encryption on the Internet, including national security risks (e.g., instructions on making bombs, illegal drug production, etc.) (Price, 1999).

The anonymity feature of ICTs, however, is a double-edged sword. The Internet's anonymity has made it possible for law-enforcement authorities to track and capture some sources of malicious activities. According to a June 2001 indictment by a US federal grand jury, two Russian hackers allegedly broke into computer systems of US banks and e-commerce sites in 10 states; stole thousands of credit card numbers and threatened the victim firms that they would not stop unless they were hired as security consultants. The anonymity feature also allowed US FBI agents to pretend as executives of an e-commerce company. They brought the hackers to the United States for job interviews and arrested (Stone, 2001).

6.4 Concluding Comments

This chapter has shed some lights on positive and negative asymmetries associated with ICTs. Such asymmetries are functions of characteristics of nations, organizations, individuals, and institutions. Libicki (2009, p. 70) observes: "Perfectly symmetric warfare does not exist, particularly when the United States is involved. Yet cyberwarfare may be more asymmetric than most."

Experts say that cyber-terrorism, which can be considered as "the marriage of terrorism and cyberspace" has been relatively absent in the world (Gabrys, 2002). Although negative asymmetries created by ICTs cannot be completely eliminated, they can, at least, be lessened (Metz, 2001). The world will be more secure if measures are taken at various levels to minimize vulnerabilities associated with negative asymmetries. These asymmetries are related to direct or first degree threats ranging from simple viruses to sophisticated cyber-terrorism, and indirect or second degree threats such as use of ICTs for secure communication by terrorists.

Finally, international competitiveness of a nation in the digital age is a function of its capability to ensure national security. Various sources of positive and negative asymmetries discussed in this chapter provide insight into the ICT-national security nexus.

Notes

1. Nemets and Torda (2001) report that Russian organized crime groups were supplying nuclear, biological, and chemical warfare technologies as well as other sophisticated asymmetric technologies to Al Qaeda in exchange of Afghan heroin.
2. See Bank Technology News (2003). Security: Biometrics takes hold overseas: Significant hurdles remain to adoption in the US 16(12) (December): 10.
3. The "Red Hacker Alliance" is arguably the largest and earliest hacking group in China. An estimate suggested that it had 20,000 hackers in 2005, which has about 80,000 registered members at the peak (crime-research.org, 2005).
4. Also see "Material handling news article" http://www.mhmonline.com/nID/2957/MHM/viewStory.asp.
5. The "Storm Cloud" is a US spy investigation case. During 1998–2000, hackers that were traced back to Russia allegedly downloaded a huge mass of sensitive data that included one colonel's entire e-mail inbox and hacked the US Defense Department computers, among others (Bridis, 2001).
6. Online casinos rely on Worldpay to process customer's transactions and pay off gamblers (Walker, 2004).

References

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

Aggarwal, V. (2009, August 3). Lead: Cyber crime's rampant. *Express Computer*. http://www.expresscomputeronline.com/20090803/market01.shtml. (Accessed 22 October 2009).

Baron, W. R. (1997, Spring). Volpe engineers use biometrics to help ease border crush. *Volpe Journal*, available at: http://www.volpe.dot.gov/infosrc/journal/spring97/biomet.html (Accessed 22 October 2009).

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

Blank, S. (2004). Rethinking the concept of asymmetric threats in US strategy. *Comparative Strategy, 23*(4/5), 343–367.

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

Bridis, T. (2001, June 27). E-Espionage rekindles cold-war tensions – US tries to identify hackers; millions of documents are stolen. *Wall Street Journal,* A.18.

Bronk, C. (2009). Time to move toward a more secure cyberspace. *World Politics Review*. http://www.worldpoliticsreview.com/article.aspx?id=4194

Bucci, C., & Steven, P. (2009). A most dangerous link. *US Naval Institute Proceedings, 135*(10), 38–42.

Busetta, A., & Milito, A. M. (2009). Socio-demographic vulnerability: The condition of Italian young people. *Social Indicators Research*. DOI 10.1007/s11205-009-9507-9.

Coll, S. (2008). *The Bin Ladens: An Arabian family in the American century*. New York: The Penguin Press.

crime-research.org. (2005, May 3). Red Hackers come back! http://www.crime-research.org/news/03.05.2005/1199. (Accessed 22 October 2007).

Denning, D. E. (2003). Chapter eight: Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy*. Rand Corporation Monograph/Report MR-1382. http://www.rand.org/pubs/monograph_reports/MR1382/index.html. (Accessed 22 October 2008).

The Economist. (2008a, December 8). Marching off to cyberwar. *389*(8609), 20.

The Economist. (2008b). Between Allah and America. *387*(8575), 92–93.

English, L. P. (2005). Information quality: Critical ingredient for national security. *Journal of Database Management, 16*(1), 18–32.

Fisher, I. (2002, August 1). Cybercafe crackdown may trip up leering boys. *New York Times*.

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

GAO Reports. (2007, June 22). *Public and private entities face challenges in addressing cyber threats*. RPT-number: GAO-07-705.

Garner, J. M. (1997, March). Asymmetric niche warfare. *Phalanx*, 1.

Gillis, C., & McHugh, M. (2002, February). Bonner proposes 'smart box'. *American Shipper*, 33.

Gotz, G. (1999). Monopolistic competition and the diffusion of new technology. *The Rand Journal of Economics, 30*(4), 679–693.

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

Harris, C. (2009, October 6). Making cyber-security a national priority. *Government Technology Magazine*. http://www.govtech.com/dc/articles/714308. (Accessed 22 October 2009).

Harvard Law Review. (2006, June). Note: Immunizing the Internet, Or: How I learned to stop worrying and love the worm, *119*, 2442.

Hernandez, J. C., Sierra, J. M., & Ribagorda, A. (2004). Beware of the security software. *Information Systems Security, 12*(6), 39–45.

Hirsh, M. (2002). Bush and the world. *Foreign Affairs, 81*(5), 18–44.

Hoo, K. S., Goodman, S., & Greenberg, L. (1997). Information technology and the terrorist threat. *Survival, 39*(3), 135–155.

Jesdanun, A. (2008, April 6). US cyberwarfare prep includes offense. http://news.yahoo.com/s/ap/20080406/ap_on_hi_te/cyberwarfare. (Accessed 22 October 2009).

Johnson, M. L. (2004, April). Biometrics and the threat to civil liberties. *Computer*, 90–93.

Kelley, J. (2001, February 5). Terror Groups Hide Behind Web Encryption, USA Today, http://www.usatoday.com/tech/news/2001-02-05-binladen.htm. Accessed 20 March 2010.

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

Lane, M. (2005, February 2005). Customs reform and trade facilitation: An entrée to the global marketplace. *USAID*. http://tcb-fastrade.com/downloads/IP_Customs_Reform_S.pdf. (Accessed 22 October 2006).

Lenzner, R., & Vardi, N. (2004, September 20). The next threat. *Forbes*, 70.

Liang, Q., & Xiangsui, W. (1999, February). *Unrestricted warfare.* Beijing: PLA Literature and Arts Publishing House. http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf. (Accessed 22 October 2004).

Libicki, M. C. (2009). Cyberdeterrence and cyberWar, a report prepared for the United States Air Force. *The RAND Corporation*. http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf. Accessed 27 October 2009.

Maltz, M. (2009,October 21). Turning power lines into battle lines. *The National Post*. http://network.nationalpost.com/np/blogs/fullcomment/archive/2009/10/21/milton-maltz-turning-power-lines-into-battle-lines.aspx (Accessed 22 October 2009).

Maney, K. (2001). Osama's messages could be hiding in plain sight. *USA Today*, B6.

McGeer, B. (2002). Security: Bankers fight a new battle it adjustments, purchases Part of Patriot Act. *Bank Technology News*, 15(11), 1.

McHugh, M., & Damas, P. (2002, November). Mega-port groups back security pilot. *American Shipper*, 14–18.

Meigs, M. C. (2003). Unorthodox thoughts about asymmetric warfare. *Parameters, 33*(2), 4–18.

Metz, S. (2001, July–August). Strategic asymmetry. *Military Review, 81*(4), 23–31.
Metz, S., & Johnson, D. V., II. (2001, January). *Asymmetry and US military strategy: Definition, background, and strategic concepts.* Carlisle Barracks, PA: US Army War College, Strategic Studies Institute.
Michael, G. (2009). Adam Gadahn and Al-Qaeda's internet strategy. *Middle East Policy, 16*(3), 135–152.
Nance, M. (2008, May/June). How (not) to spot a terrorist. *Foreign Policy, 166*, 74–76.
Nemets, A., & Torda, T. (2001, November 9). Interesting cards up Putin's sleeve: Russian sponsorship of international terrorism. *newsmax.com*. http://www.newsmax.com/archives/articles/2001/11/9/143709.shtml. (Accessed 22 October 2009).
Onlinecasinonews.com. (2004, February 3). Mob's extortion attempt on Internet bookies. http://www.onlinecasinonews.com/ocnv2_1/article/article.asp?id=4748. (Accessed 22 October 2005).
Price, S. A. (1999). Understanding contemporary cryptography and its wider impact upon the general law. *International Review of Law, Computers & Technology, 13*(2), 95–126.
Reid, T. (2007). China's cyber army is preparing to march on America, says Pentagon. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece. (Accessed 22 October 2008).
Robertson, J. (2007, November 30). China disputes report calling it a key cyber warfare instigator. *The Age*, http://news.theage.com.au/technology/china-disputes-report-calling-it-a-key-cyber-warfare-instigator-20071130-1dwx.html. Accessed 20 March 2010.
Rogers, E. M. (1983). *The diffusion of innovations* (3rd ed.). New York: Free Press.
Rogers, E. M. (1995). *The diffusion of innovations* (4th ed.). New York: Free Press.
Rosenberger, J. D. (2005). The inherent vulnerabilities of technology. *The Wargames Directory*. http://www.wargamesdirectory.com/html/articles/Various/technology.asp. (Accessed 22 October 2006).
Sabel, C., & Zeitlin, J. (eds.) (1997). *World of possibilities: Flexibility and mass production in western industrialization*. New York: Cambridge University Press.
Scott, W. R. (1995). *Institutions and organizations*. Thousand Oaks, CA: Sage.
Scott, W. R. (2001). *Institutions and organizations*. Thousand Oaks, CA: Sage.
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.
Spartacus (UD) Spartacus educational, http://www.spartacus.schoolnet.co.uk/FWWmaximgun.htm. Accessed 22 October 2009.
Stone, B. (2001, July 16). Busting the web bandits. *Newsweek*, 55.
Storper, M., & Walker, R. (1989). *The capitalist imperative: Territory, technology and industrial growth.* London: Basil Blackwell.
Swartz, J. (2007, March 12). Chinese hackers seek US access; Attacks highlight weaknesses in Internet security. *USA Today*, 3B.
Sudworth, J. (2009). New 'cyber attacks' hit S Korea. *BBC News*. http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm. (Accessed 22 October 2009).
Thomas, T. L. (1999, September–October). Infosphere threats. *Military Review*. Posted on: Foreign Military Studies Office. http://fmso.leavenworth.army.mil/fmsopubs/issues/infosphere/infosphere.htm. (Accessed 22 October 2005).
United States Government Accountability Office. (2007). Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats: GAO-07-705, June. http://www.gao.gov/htext/d07705.html. (Accessed 22 October 2008).
Vardi, N. (2005, July 25). Chinese take out. *Forbes*, 54.
Varese, F. (2002). *The Russian Mafia: Private protection in a new market economy*. New York: Oxford University Press.

Verton, D. (2003). *Black ice: The invisible threat of cyberterrorism.* New York: McGraw-Hill/Osborne.

Walker, C. (2004, June). Russian Mafia Extorts Gambling Websites. http://www.americanmafia.com/cgi/clickcount.pl?url=www.americanmafia.com/Feature_Articles_270.html. (Accessed 22 October 2005).

Waller, J. M. (2000, February 28). PLA revises the art of war. *Insight on the News,* 21–23.

World IT Report. (2003, February 3). Pakistan faces difficulties to block porn sites.

World Tribune. (2008). Pentagon official: China may already be at cyberwar with US March 13. http://www.worldtribune.com/worldtribune/WTARC/2008/ea_china_03_13.asp. (Accessed 22 October 2009).

Young, J. (2004). BC attempts to regulate international outsourcing of personal information. *Deeth Williams Wall LLP*. http://www.dww.com/articles/bcpatriot_amendments.htm. (Accessed 22 October 2005).

Yousafzai, S., & Hirsh, M. (2004). The harder hunt for Bin Laden. *Newsweek*, December 29, 2003/January 5, 2004, 58.

Zhou, L. (2005). Special Issue: Database technology for enhancing national security. *Journal of Database Management, 16*(1), I–III.

Zombori, G. (2001, January 5). *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. http://www.yorku.ca/nathanson/Publications/e.htm. (Accessed 22 October 2009).