Information and communications technologies, strategic asymmetry and national security

By: Nir Kshetri

Kshetri, Nir (2005), "Information and Communications Technologies, Strategic Asymmetry and National Security," *Journal of International Management*, 11(4), *563-580*.

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 article discusses various asymmetries associated with institutions, nations and organizations that influence the ICT-national 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. Integrative approaches that combine policy and technological measures at various levels are likely to make the world more secure.
Keywords: Strategic asymmetry; Information and communication technologies; National security; Institutions; Cyber attacks

Article:

1. Introduction

Information and communications technologies (ICTs) play a critical role in the national security game (e.g., English, 2005; Metz, 2001; Zhou, 2005). The vulnerability to threat as well as the capability to strategically deploy ICTs vary across entities. The characteristics of organizations, nations and institutions superimpose in a unique interaction with ICTs' nature that influence the ICT-security nexus.

The focus of this paper is on asymmetry (see Table 1 for definitions of terms) associated with ICTs from the perspective of national 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., cyber attacks) 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, etc. 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 2).

In the history of warfare, there are several examples[1] of strategic uses of asymmetric technologies (Metz, 2001) that have provided "a decisive advantage over an opponent in combat" (Rosenberger, 2005). 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 U.S. investigators to convert huge amount of data into actionable intelligence. The intelligence helped to track the wanted Iraqis. Analyst's Notebook also helped to trace the creator of "love bug' computer virus of 2000 (Yousafzai and Hirsh, 2004). U.S. military and intelligence officials are using the same technology to track Osama Bin Laden's network. Bin Laden's network, on the other hand, has been reportedly using symmetric and asymmetric technologies[2] including satellite phones, the Internet and advanced encryption methods to recruit followers, raise money, formulate plans and operations and to

communicate securely (see Box 1).

Table 1
Explanation of major terms used in the paper

Term	Explanation
Encryption technologies[a]	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[b]	These include telecommunications as well as digital technologies such as telephony, cable, satellite, radio, computers, information networks and software.
Negative asymmetry[c]	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".[d]
Positive asymmetry[c]	Capitalizing on differences to gain an advantage.
Steganography[c]	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[c]	The advantage that can result from matching the opponent in terms of strategic resources.
Strategic asymmetry[c]	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[f]	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[g]	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 http://www.loansnap.com/security.htm.
[b] See http://www.google.com/url?sa=X&start=0&oi=define&q=http://www.cyber.law.harvard.edu/readinessguide/glossary.html.
[c] Metz (2001), Metz and Johnson (2001).
[d] See http://www.en.wikipedia.org/wiki/National_security.
[e] Maney (2001), Hernandez et al. (2004).
[f] http://www.allshredservices.com/faq/grammleachbliley.htm.
[g] Young (2004).

Table 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	• Cyber attacks on critical infrastructures	• Communications (e.g., AL Qaeda's encrypted e-mails) • Detection of threats from enemies (Smart containers in U.S. 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

The objective of this paper is to explore the nature of ICT-related asymmetries of organizations, nations and individuals that influence national security. The remainder of the paper is structured as follows: The next section discusses some positive and negative asymmetries that ICT tools can create. Then, we develop some propositions on institutional and organizational factors linked with positive and negative asymmetries. Finally, we provide managerial and policy implications and suggest directions for future research.

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. 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 ICTcreated 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 U.S. because of their technology advanced research (Bridis, 2001) as well as capabilities to combine ICTs with non-ICT resources.

Box 1
Al Qaeda's amazingly advanced Internet network

Experts believe that critical U.S. infrastructures such as energy, transportation, water, and telecomm are highly susceptible to Al Qaeda's cyber attacks. 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 U.S. economy by penetrating the computer networks of major companies. Although no cyber attack has yet been traced to Al Qaeda, this outfit's network use has been amazingly sophisticated.

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 the San Francisco Chronicle on October 6, 2001, Al Qaeda has recruited talented software engineers to achieve its Internet ambition.

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.

U.S. officials have reported that Bin Laden's 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 U.S. airliners. Similarly, a suspect in the bombings of U.S. 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 U.S.

Al Qaeda's integration of encryption with steganography has been a real challenge to U.S. 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.

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 U.S. military combines training and leadership (non-ICT resources) with ICTs to gain and sustain its superiority (Metz, 2001). During 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 Al Santoli, editor of the China Reform Monitor, senior colonels of the Chinese military Qiao Liang and Wang Xiangsui, in their 1999 book, Unrestricted Warfare have argued that since China's People's Liberation Army (PLA) lacks resources to compete with the U.S. 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" (Waller, 2000). The authors have urged on the development of a means of challenging the U.S. through asymmetry rather than matching the U.S. in terms of all types of resources (Waller, 2000).

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 U.S.- 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 U.S.) and regulative institutions (e.g., a potential threat of lawsuit for failing to protect patients' information).

Table 3
Propositions on institutional and organizational factors linked with positive and negative asymmetries

Proposition	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)	

IV=independent variable; DV=dependent variable.

Negative asymmetry involves "an opponent's threat to one's vulnerabilities" (Metz, 2001). 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 U.S. counterterrorism organizations. Similarly, a suspect in the bombings of the U.S. embassies in Kenya and Tanzania in 1998 reportedly sent encrypted e-mails under various names (Kelly, 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 U.S. airliners.

3. Institutional and organizational factors linked with positive and negative asymmetries

Table 3 summarizes our propositions on institutional and organizational factors linked with positive and negative asymmetries associated with ICTs. In Propositions 1 and 2, potential positive and negative asymmetries created by business models are dependent variables and regulative legitimacy to such models is an independent variable. Propositions 3–8 have positive and negative asymmetries as dependent variables and constructs related to institutional and organizational factors as independent variables. As indicated in Table 3 some of the propositions are specific to certain deploying units such as a government and criminal groups. Table 4 explains these relationships in more details with some examples.

Table 4
Some sources of ICT-led asymmetries

Source of asymmetry	Explanation	Remarks/examples
Institutions		
Regulatory	• Strength of the rule of laws.	• The lack of laws against cyber attacks and the lack of existence of enforcement mechanisms increase positive asymmetries of cyber criminals.
	• Laws to minimize vulnerability to negative asymmetries.	• The Patriot act in the U.S. and China's regulation regarding encryption software.
	• Laws directed toward minimizing symmetric advantages of adversaries.	• Laws dealing with the export of encryption products (also COCOM restriction).
Normative	• Social obligations.	• ACLU in the U.S.
	• Professional obligations.	• Honker Union (Red Hackers) of China
Cognitive	• Perception of threat.	• China's interpretation of military security associated with ICT import.
	• Perception of adversaries' capability.	• Chinese military's interpretation of U.S. 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 others.	• 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.

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 and Walker, 1989; Sabel and Zeitlin, 1997). Various asymmetries to a unit arise by default because of the nature of the institutions in which the unit is embedded. Viewing from a "rational perspective', institutions are mechanisms that provide efficient solutions to predefined problems (e.g., a terrorist organization's choice of media to spread its propaganda; the Mafia group's choice of a website to attack, etc.). 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.

Scott (1995, 2001) has conceptualized institutions as composed of three broad categories— regulative, cognitive, and normative (see Table 4). These components influence institutional preference for employing ICTs to create positive and negative asymmetries. Each set has corresponding legitimacy concerns.

3.1.1. Regulative institutions

Kelman (1987) argues that regulative institutions focus on the pragmatic legitimacy concerns in managing the demands of regulators and governments. In the context of this paper, regulative institutions consist of regulatory bodies (such as the U.S. Department of Homeland Security) and the existing laws and rules (e.g., the Patriot Act and the Gramm–Leach–Bliley (GLB) Act in the U.S.) that influence individuals and organizations to behave in certain ways. Individuals and organizations adhere to the rules so that they would not suffer the penalty for noncompliance (Hoffman, 1999).

First, there are international differences in terms of laws to minimize vulnerability to several forms of negative asymmetries. U.S. government, for instance, requires commercial banks to secure their networks. The Patriot Act and the Gramm–Leach–Bliley (GLB) Act (Table 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 U.S. 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 U.S. and China. We propose that:

Proposition 1. *Ceteris paribus,*[3] *ICT associated business models that increase negative asymmetries of governments and citizens are less likely to gain regulative legitimacy.*

Second, nations across the world differ in terms of laws directed toward maintaining positive asymmetries. For instance, until the late 1990s, the U.S. 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 towards specific sources of threat. In the 1980s, national security concerns from the

U.S. 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 U.S. 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 U.S. 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 U.S. companies during 1996–1998, with the approval of the Department of Commerce. The next proposition is:

Proposition 2. *Governments are less likely to provide regulative legitimacy to business models that allow adversaries to create positive asymmetry.*

Third, nations across the world differ drastically 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. By the end of 2000, only about 45 nations in the world had laws recognizing and validating some forms of digital or electronic signatures and transactions. For instance, when a Filipino hacker launched the "Love Letter" virus in 2000, estimated loss of damage in the U.S. was in the range of $4–15 billion. However, the U.S. government could not do anything to prosecute the hacker or to recover the damages because at that time the Philippines had no laws prohibiting such crimes (Adams, 2001). Some nations that have enacted laws against computer crimes, on the other hand, lack enforcement mechanisms. For instance, Indonesia is one of the top nations in terms of cyber frauds thanks to the lack of expertise and resources of Indonesian police to combat cybercrimes (Darmosumarto, 2003; de Kloet, 2002; Tedjasukmana, 2002).

Likewise, too weak state (Varese, 2002), inefficient police[4] 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 and Bush, 2005). Experts also argue that law enforcement officials in countries like China and Russia don't 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 and Johnson, 2001). The discussion above is summarized as:

Proposition 3. *The lack of strong rules of law increases cyber criminals' ICT-created positive asymmetry.*

3.1.2. Normative institutions

Normative components introduce "a prescriptive, evaluative, and obligatory dimension into social life" (Scott, 1995, p. 37). Normative institutions include trade associations, professional associations (e.g., the Honker Union of China, also known as the Red Hackers), or non-profit organizations (e.g., ACLU in the U.S.) that can use social obligation requirements to induce certain behavior.

The basis of compliance in the case of normative institutions derives from social obligations, and non-adherence can result in societal and professional sanctions. For the purpose of this paper, the normative component focuses on the values and norms held by individuals, organizations and government agencies that influence the ICT-national security nexus.

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. For instance, Verton (2003), pointing out vulnerabilities of unprotected

wireless networks in hospitals, 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 towards 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 U.S. 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 biometrics thus reduces 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 U.S. and European countries, for instance, have different views on privacy protection. In the U.S., it is argued that identification systems based on face-recognition technology pose civil liberty threats (Johnson, 2004). U.S. Banks feel more obligated to protect personal privacy of their patrons than their European counterparts. For this reason, U.S. banks are slower to adopt biometric products in a range of services. Most European Union (EU) nations, on the other hand, include biometric fingerprints in national drivers' licenses.

In 2003, 14 U.S. 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 U.S., the lobbying and efforts of organizations like the American Civil Liberties Union (ACLU) played key roles in the failure of the bills.[5]

Professional organizations such as the Honker Union of China (also known as the Red Hackers) 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 U.S. warplane. On May 1, 2001, a Chinese hacking group publicly released its plans for a "Net War", which was planned to continue until the anniversary of the bombing (May 7). In response, hacking groups from the U.S., Brazil and Europe attacked Chinese websites. According to an article published in NewMax.com Wires[6] Chinese hackers attacked 1100 U.S. sites while American hackers broke into 1600 Chinese sites. The above leads to the following:

Proposition 4. *The strength of normative legitimacy influences: a) the ability to use ICTs to create positive asymmetry; and b) the ability to deal with vulnerabilities of negative asymmetries.*

3.1.3. Cognitive institutions

Scott (1995) suggests that "cognitive elements constitute the nature of reality and the frames through which meaning is made". Although carried by individual members, cognitive programs are elements of the social environment. Cognitive institutions are associated with culturally supported habits and exert subtle influences on ICT deployment for proactive security, defense, and protection efforts.

Cognitive institutions affect the way people notice, categorize, and interpret stimuli. To take an example, there has been a deep rooted perception among Chinese policy makers that Microsoft and the U.S. government spy on Chinese computer users through secret "backdoors" in Microsoft products.[7] Several years ago, Chinese cryptographers reportedly found an "NSA Key" in Microsoft products, which was interpreted as the National Security Agency. The key allegedly provided the U.S. government backdoor 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. An article published in China Economic Times on June 12, 2000 discussed three mechanisms that Xu Guanhua, then Chinese vice minister of the science and technology, thought high technology affects national security—military security, economic security, and cultural security.

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

Some U.S. observers, on the other hand, think that countries like China, Russia and North Korea are systematically probing the computer networks in the U.S. to find weaknesses that can be exploited (Bickers, 2001). A group of U.S. defense analysts also argued that the growing use of Linux (open source software) in U.S. defense systems presents an urgent national security threat. They have maintained that Linux companies have deployed development centers with programmers from China and Russia, on one hand, and open nature of Linux enables hackers or cyber-terrorists to exploit the system, on the other.

As we 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 U.S. military's capability to assimilate ICTs in warfare. The authors of Unrestricted Warfare, for example, have observed that the U.S. 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). Thus, we propose that:

Proposition 5. *Perception of ICT-related security threats from an adversary results in the government's measures to employ ICTs in: a) creating positive asymmetries; b) dealing with vulnerabilities of negative asymmetries.*

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 4).

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) in industrial economics literature. Japan, for instance, has planned to introduce 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 U.S., 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.[8]

Whereas industrialized countries are rapidly adopting ICTs to create positive asymmetries and to counter negative asymmetries, 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 and 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 (McHugh and Damas, 2002).9 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, new laws in Pakistan require Internet cafe´s to check their clients' identity cards (Fisher, 2002) and Internet users are not allowed to use encryption technology.10 Nonetheless, these laws have largely been ignored (World IT Report, 2003). Thus:

Proposition 6. *ICT deployment to create positive asymmetries and deal with negative asymmetries varies positively with the level of economic development of a nation.*

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 cyber attacks (Kshetri, 2005). A high dependence on digital technologies is a weakness that adversaries can exploit. Garner (1997, p. 1) observes:

> 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).

An estimate suggested that U.S. banks spent US$60 million in 2002 on technology to comply with the requirements of the Patriot Act (McGeer, 2002). According to an article published in Computerworld on September 27, 2004, hackers that were involved in mass attacks before are moving towards more focused attacks that target mainly e-commerce sites. Another study by IDC indicated that over 60% of computer attacks targeted[11] financial institutions in 2003 (Swartz, 2004). Similarly, in the first half of 2004, 16% of e-commerce attacks were targeted compared to 4% in 2003 (Symantec, 2004).

To some extent, rank effect discussed in the previous section also holds true for vulnerabilities to threat. Cyber attacks, for instance, are more likely to be targeted to developed countries with large networks such as the U.S. than developing countries. For instance, Dan Verton, 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 U.S. economy by breaking encryption algorithms and infiltrating the technological systems of major corporations". Thus:

Proposition 7. *A higher degree of dependence on digital technologies increases a nation's vulnerability to ICT related negative asymmetry.*

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 (Bridis, 2001). 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,[12] U.S. 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[13] on Worldpay[14] System that affected thousands of online casinos. The website of VIP Management Services was first targeted in September 2003 and was regularly attacked since then (Walker, 2004). In the early, 2004, the company reportedly received e-mails demanding $30,000 via Western Union (Onlinecasinonews.com, 2004).

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 the video 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 U.S. federal grand jury, two Russian hackers allegedly broke into computer systems of U.S. 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 U.S. FBI agents to pretend as executives of an e-commerce company. They brought the hackers to the U.S. for job interviews and arrested (Stone, 2001). Based on the above, a final proposition is:

Proposition 8. *The degree of ICT-created positive asymmetries is higher for an adopting unit that has a higher importance of anonymity functions.*

4. Managerial and policy implications and directions for further research

This paper has provided theoretical and some empirical understanding of positive and negative asymmetries associated with ICTs. We found that such asymmetries are functions of characteristics of nations, organizations, individuals and institutions.

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.

Implication 1. *Organizations must be vigilant to ensure that measures are taken to deal with governments', organized criminals' and individuals' ICT-created positive and negative asymmetries.*

Regulatory landscape influencing the cybercrime industry is changing very rapidly. New laws may force companies to change business models to minimize nations' and citizens' negative asymmetries as well as to restrict adversaries (e.g., terrorists and hostile nations) from gaining symmetric advantages. Just like the U.S. Patriot Act's requirement for banks to spend on technology to enhance security, compliance with new laws written for electronic criminal activity may provide similar pressure.

Ensuring that both technological and behavioral/perceptual factors are given equal consideration in the design and implementation of a computer network is crucial. Technological measures range from simply disconnecting databases containing sensitive information from the Internet to the deployment of sophisticated antifraud technologies. Similarly, simple behavioral measures can stop some serious cybercrimes. For instance, a study conducted by MailFrontier in the early 2003 indicated that 40% of people who read a fraudulent Citibank e-mail considered it as a real one (Salkever, 2003). A simple training strategy aimed at improving the ability of employees to distinguish a fraudulent e-mail with a real one may reduce a significant proportion of such crimes.

Implication 2. *ICT and competitive strategies such as outsourcing should go beyond obvious considerations such as core competence, human resource and service quality (e.g., Goo et al., 2000).*

For instance, origination and destination countries in offshore business process outsourcing may differ on regulative, normative, and cognitive institutions. In some cases, such differences can translate to negative asymmetries for a party. The Pakistani medical transcriber discussed earlier took advantage of institutional

differences in the U.S. (outsourcing origination) and Pakistan (destination). Such differences produced negative asymmetry for the U.S. hospital and positive asymmetry for the Pakistani medical transcriber. Each move that involves ICT should be evaluated in terms of new vulnerabilities that adversaries can exploit.

Implication 3. *All firms are not equally susceptible to the vulnerability of ICT-created security risks.*

Some firms are more affected than others by governments', organized criminals' and individuals' measures to use ICTs to create positive asymmetries and deal with negative asymmetries. For instance, some computer hackers' interests are framed by fight against global capitalism (de Kloet, 2002). Such hackers are likely to attack networks of big multinationals. Similarly, terrorists are more likely to target the networks of sensitive organizations such as hospitals and critical infrastructures. Likewise, exploiting online casinos' dependence on Internet technologies, cyber criminals have extorted millions of dollars with them (Kshetri, 2005). A firm's management of security risks requires an understanding of its position on the spectrum of positive and negative asymmetries created by ICTs.

Implication 4. *Policy measures are needed to increase the probability of arrest of cyber criminals.*

Like other criminals (Becker, 1995), we can assume that cyber criminals are risk takers rather than being risk avoiders. Most measures taken so far have emphasized on increasing penalty rather than on increasing the probability of arrest. For instance, the U.S. Patriot Act brought cyber attacks into the definition of terrorism with new penalties of up to 20 years incarceration. The severity of punishment is important, but what is still more critical is the certainty of punishment (Becker, 1995). Conventional law enforcement authorities lack skills required in dealing with cybercrimes. The probability of arrests is likely to increase (or cyber criminals' perceived degree of positive asymmetry will decrease) with more investments in the skills of law enforcement authorities.

Implication 5. *Technology measures alone are not sufficient to deal with the vulnerabilities of ICT-created negative asymmetries.*

There have been an increasing number of attacks on computer networks notwithstanding significant investments in security.15 Integrated approaches that combine technology and policy measures are thus likely to be more successful. Important technological issues crossing national borders thus must be dealt with at policy levels (Skolnikoff, 1989). Private companies, nonprofit organizations (such as ACLU), national governments and supranational institutions can work together to deal with forces that influence global security. Especially, international institutions carry enormous power that can be harnessed to enhance global security. More than 25 years ago, Henkin (1979) observed that "almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time" (p. 47). The statement is still true but specific sets of international institutions are likely to play important roles. For instance, International Telecommunications Union (ITU) has its members as nations as well as corporations. The corporate members of ITU can influence the designs of ICTs and international security standards. In terms of harmonization of laws, the UN Commission on International Trade Law (UNCITRAL) undertook works leading to the adoption of the Model Law on E-Commerce. Many countries enacted new e-commerce laws by taking UNICITRAL modal law as the guideline. There is an urgent need for laws related to international standards for electronic money laundering, encryption technologies and cyber attack. International harmonization of such laws can influence the ICT-global security nexus.

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 paper provide insight into the ICT-national security nexus.

An important area of future research concerns testing propositions related to ICT-created positive and negative asymmetries discussed in this paper. Positivist qualitative research, which emphasizes causality, can be

employed to test the propositions (Myers, 1997; Orlikowski and Baroudi, 1991, p. 5). Especially, case studies can provide a clearer understanding of complex phenomena such as utilization of ICT tools to manage asymmetries by nation and non-nation entities. Efficacy of case study research lies in addressing research questions related to "hows" and "whys" of the complex process of ICT deployment in creating positive asymmetries and dealing with negative asymmetries (Oz, 2004; Yin, 1994, pp. 3–6). In-depth longitudinal examination of a case related to the management of ICT-related asymmetries would also reveal interesting multivariable patterns (Hitt et al., 1998).

Future research is also recommended to better understand how ICT-created asymmetry interacts with other forms of asymmetry mentioned above (e.g., method, will, morale, organization, and patience). For instance, a question related to interaction between an ICT- created asymmetry and an asymmetry related to organization is: non-state/non-nation entities organized as networks (Al Qaeda) differ from nations in terms of their capabilities to create positive asymmetries and deal with negative asymmetries.

In this paper, we discussed a number of ICT functions that contribute to create asymmetric advantages. They include employing ICT tools to fight a war against an enemy (e.g., development of cyber war technologies in some nations), communicating (e.g., Al Queda's Internet network), detecting threats from enemies (e.g., deployment of smart containers), etc. Future research is also required to construct a clearer taxonomy of ICT functions that are used to create positive asymmetries and to deal with the vulnerabilities of negative asymmetries. Furthermore, it is important to explore how different entities differ with respect to the taxonomy. Some research questions include the following: How do nations and non-nation organizations differ in terms of the taxonomy of ICT functions related to positive and negative asymmetries? How do nations at different levels of economic development differ with respect to the taxonomy?

Notes:

1 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 1893–1994 Matabele war, 50 British soldiers with just four Maxim guns fought of 5000 Matabele warriors (see http://www.spartacus. schoolnet.co.uk/FWWmaximgun.htm). Similarly, asymmetric technologies used by the U.S. Army include, cruise missiles, laser-guided bombs, satellite reconnaissance systems, high altitude reconnaissance aircraft, and unmanned aerial vehicles (Rosenberger, 2005).

2 Nemets and Torda (2001) report that Russian Mafia groups were supplying nuclear, biological and chemical warfare technologies as well as other sophisticated asymmetric technologies to Al-Qaeda in exchange of Afghan heroin.

3 All propositions are stated on a ceteris paribus — – other things being equal–basis. The phrase "ceteris paribus" is implicit at the beginning of each proposition and has not been explicitly stated.

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

5 See Bank Technology News, 2003. Security: Biometrics takes hold overseas: Significant hurdles remain to adoption in the U.S. 16(12) (December): 10.

6 See http://www.newsmax.com/archives/articles/2001/5/22/84452.shtml.

7 For example, see http://www.hknet.tm.tue.nl/section32/security.html.

8 See Volpe Engineers Use Biometrics to Help Ease Border Crush, available at: http://www.volpe.dot.gov/infosrc/ journal/spring97/biomet.html.

9 Also see "Material handling news article" http://www.mhmonline.com/nID/2957/MHM/viewStory.asp.

10 See http://www.c4group.net/ivhp/bilgibelge/docs/enemies%20of%20internet.doc.

11 Cyber attacks can be targeted or opportunistic. In targeted attacks, specific tools are used against specific cyber targets. Opportunistic attacks, on the other hand, entail releasing of worms and viruses that spread indiscriminately across the Internet. Targeted attacks are carried out by highly skilled hackers. These hackers possess expertise to do serious damage. Some of them are motivated by financial gains. Targeted attacks are also initiated by terrorists, ideological hackers or government agencies. The government of Burma, for instance, reportedly monitors online critics of the regime and sends them viruses attached in e-mails (Havely, 2000).

12 The "Storm Cloud" is a U.S. 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 U.S. Defense Department computers, among others (Bridis, 2001).
13 There are two categories of DoS attacks: Operating System (OS) attacks, and Network attacks. OS attacks entail discovering holes in the security of the OS and bringing down the system. Network attacks disconnect a network from the Internet services provider (ISP). The attackers use mis-configured networks to perform such attacks (see "Help! I am being DoS'ed" at http://www.irc-junkie.org/content/a-DoS.php).
14 Online casinos rely on Worldpay to process customer's transactions and pay off gamblers (Walker, 2004).
15 A Global Security Survey conducted by Deloitte Touche Tohmatsu in 2003, for instance, found that respondent companies spent 6% of their IT budgets on security. Nevertheless, cyber attacks have not diminished (Carblanc and Moers, 2003). With hacking technologies' advancement, technologies that try to prevent hackers from cracking into protected hosts are not bulletproof. According to IDC Worldwide IT security forecast, 39% of Fortune 500 companies in 2003 suffered a security breach and 40% of global IT managers have rated security as their number one priority. An article published in Computerworld on September 27, 2004 quotes Symantec's Internet security Threat Report, which indicated that for the first six months of 2004, 48 new vulnerabilities per week were announced.

References

Adams, J., 2001. Virtual defense. Foreign Affairs, 98–112 (May/Jun).
Becker, G.S., 1995. The economics of crime. Cross Sections, 8–15 (Fall, http://www.rich.frb.org/pubs/cross/crime/ crime.pdf).
Bickers, C., 2001. Combat on the Web. Far Eastern Economic Review 16, 30–33 (August).
Blau, J., 2004. Russia—a happy haven for hackers, 26 May 2004. http://www.computerweekly.com/Article130839.htm. Bridis, T., 2001. E-espionage rekindles cold-war tensions—U.S. tries to identify hackers; millions of documents are stolen. Wall Street Journal, A.18 (Jun 27).
Carblanc, A., Moers, S., 2003. Towards a culture of online security. OECD Observer, 30. (December 2003).
Darmosumarto, S., 2003. Battle on Internet credit card fraud still long. Jakarta Post (December 08, http://www.crimeresearch.org/news/2003/12/Mess0802.html).
de Kloet, J., 2002. Digitisation and its Asian discontents: the Internet, politics and hacking in China and Indonesia. First Monday 7 (9) (URL: http://www.firstmonday.org/issues/issue7_9/kloet/index.html).
English, L.P., 2005. Information quality: critical ingredient for national security. Journal of Database Management 16 (1), 18–32.
Fisher, I., 2002. Cybercafe crackdown may trip up leering boys. New York Times, August 1, p. 4. Section A.
Garner, J.M., 1997. Asymmetric niche warfare. Phalanx 30 (1), 1.
Gillis, C., McHugh, M., 2002. Bonner proposes `smart box'. American Shipper, 33 (February).
Goo, J., Kishore, R., Rao, H.R., 2000. A content-analytic longitudinal study of the drivers for information technology and
systems outsourcing. Proceedings of The Twenty First International Conference on Information Systems.
Gotz, G., 1999. Monopolistic competition and the diffusion of new technology. The Rand Journal of Economics 30 (4), 679–693.
Grow, B., Bush, J., 2005. Hacker hunters. Business Week, 74. May 30.
Havely, J., 2000. When states go to cyber-war, BBC News, 16 February. http://news.bbc.co.uk/hi/english/sci/tech/ newsid_642000/642867.stm.
Henkin, L., 1979. How Nations Behave. Council on Foreign Relations, New York.
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.
Hitt, M., Harrison, J., Ireland, R.D., Best, A., 1998. Attributes of successful and unsuccessful acquisitions of US firms. British Journal of Management 9, 91–114.
Hoffman, A.J., 1999. Institutional evolution and change: environmentalism and the U.S. chemical industry. Academy of Management Journal 42 (4), 351–371.
Johnson, M.L., 2004. Biometrics and the threat to civil liberties. Computer, 90–93 (April).

Kelly, J., 2001. Terror groups hide behind web encryption. USA Today (February 15).
Kelman, S., 1987. Making Public Policy: A Hopeful View of American Government. Basic Books, New York.
Kshetri, N., 2005. Hacking the odds. Foreign Policy, 93 (May/June).
Lane, M., 2005. Customs reform and trade facilitation: an entre´e to the global marketplace USAID, February 2005, http:// www.tcb-fastrade.com/downloads/IP_Customs_Reform_S.pdf.
Maney, K., 2001. Osama's messages could be hiding in plain sight. USA Today, B6 (December 19).
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. Mega-port groups back security pilot. American Shipper, 14–18 (November).
Meigs, M.C., 2003. Unorthodox thoughts about asymmetric warfare. Parameters 33 (2), 4–18.
Metz, S., 2001. Strategic asymmetry. Military Review, 23–31 (July–August).
Metz, S., Johnson II, D.V., 2001. Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts. US Army War College. Strategic Studies Institute, Carlisle Barracks, PA. January.
Myers, M., 1997. Critical Ethnography in Information Systems, in Information Systems and Qualitative Research. In: Lee, A.S., Liebenau, J., DeGross, J.I. (Eds.). Chapman & Hall, London, pp. 276–300.
Nemets, A., Torda, T., 2001. Interesting cards up Putin's sleeve: Russian sponsorship of international terrorism, www.newsmax.com, November 9, http://www.newsmax.com/archives/articles/2001/11/9/143709.shtml.
Onlinecasinonews.com 2004. Mob's extortion attempt on Internet bookies, February 3, http://www.onlinecasinonews.
com/ocnv2_1/article/article.asp?id=4748.
Orlikowski, W.J., Baroudi, J.J., 1991. Studying information technology in organizations: research approaches and assumptions. Information Systems Research 2, 1–28.
Oz, O., 2004. Using Boolean- and fuzzy-logic-based methods to analyze multiple case study evidence in management research. Journal of Management Inquiry 13 (2), 166–179.
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.
Rogers, E.M., 1983. The Diffusion of Innovations, 3rd edn. Free Press, New York.
Rogers, E.M., 1995. The Diffusion of Innovations, 4th edn. Free Press, New York.
Rosenberger, J.D., 2005. The inherent vulnerabilities of technology. The Wargames Directory, http://www.wargamesdirectory.com/html/articles/Various/technology.asp.
Sabel, C., Zeitlin, J. (Eds.), 1997. World of Possibilities: Flexibility and Mass Production in Western Industrialization. Cambridge University Press, New York.
Salkever, A., 2003. "Phishing" is foul on the Net, October 21, http://www.businessweek.com/technology/content/ oct2003/tc20031 021_8711_tc047.htm.
Scott, W.R., 1995. Institutions and Organizations. Sage, Thousand Oaks, CA.
Scott, W.R., 2001. Institutions and Organizations. Sage, Thousand Oaks, CA.
Skolnikoff, E.B., 1989. Technology and the world tomorrow. Current History 88 (534), 5–13.
Stone, B., 2001. Busting the Web bandits. Newsweek, 55 (July 16).
Storper, M., Walker, R., 1989. The Capitalist Imperative: Territory, Technology and Industrial Growth. Basil Blackwell, London.
Swartz, J., 2004. Crooks slither into Net's shady nooks and crannies crime explodes as legions of strong-arm thugs, sneaky thieves log on. USA Today, October 21, http://www.usatoday.com/printedition/money/20041021/cybercrimecover.art.htm.
Symantec, 2004. Symantec Internet Security Threat Report, vol. VI. http://www.4law.co.il/L138.pdf.
Tedjasukmana, J., 2002. The no-payment plan: thousands of young Indonesians commit cyberfraud for fun and profit.
Time (September 23, http://www.time.com/time/globalbusiness/article/0,9171,1101020923-351237,00.html).
Thomas, T.L., 1999. Infosphere threats, Military Review, September–October, Posted on: Foreign Military Studies
Office, http://www.fmso.leavenworth.army.mil/fmsopubs/issues/infosphere/infosphere.htm.
Vardi, N., 2005. Chinese take out. Forbes, 054. (July 25).
Varese, F., 2002. The Russian Mafia: Private Protection in a New Market Economy. Oxford University Press,

New York.
Verton, D., 2003. Black Ice: The Invisible Threat of Cyberterrorism. McGraw-Hill/Osborne.
Walker, C., 2004. Russian Mafia Extorts Gambling Websites, June, http://www.americanmafia.com/cgi/clickcount. pl?url=www.americanmafia.com/Feature_Articles_270.html.
Waller, J.M., 2000. PLA revises the art of war. Insight on the News, 21–23 (February 28).
World IT Report, 2003. Pakistan faces difficulties to block porn sites, February 3.
Yin, R.K., 1994. Case Study Research: Design and Methods. Sage, Thousand Oaks, CA.
Young, J., 2004. BC Attempts to Regulate International Outsourcing of Personal Information, Deeth Williams Wall LLP, http://www.dww.com/articles/bcpatriot_amendments.htm.
Yousafzai, S., Hirsh, M., 2004. The harder hunt for Bin Laden. Newsweek, 58 (December 29, 2003/January 5).
Zhou, L., 2005. Special issue: database technology for enhancing national security. Journal of Database Management 16 (1), I–III.