Cyber-threats and cybersecurity challenges: A cross-cultural perspective

By: Nir Kshetri and Lailani Laynesa Alcantara

Kshetri, Nir, and Alcantara, Lailani Laynesa (2015). "Cyber-threats and cybersecurity challenges: A cross-cultural perspective", Nigel Holden, Snejina Michailova and Susanne Tietze (Eds) *The Routledge Companion to Cross-Cultural Management*, London and New York: Routledge.

Made available courtesy of Routledge: https://doi.org/10.4324/9780203798706

This is an Accepted Manuscript of a book chapter published by Routledge in *The Routledge Companion to Cross-Cultural Management* on 24 April 2015, available online: http://www.routledge.com/9780415858687

Abstract:

As is the case of any economic activity, cultural factors are tightly linked to cybercrimes, cyberattacks and cybersecurity. Just like any other activities, some forms of cybercrime may be more acceptable in some cultures than in others. For some categories of cyberoffenses, cultural factors appear to play more important roles than other environmental factors. For instance, cybercrimes are more justifiable in some cultures. Quoting a Russian hacker-turned-teacher, Blau (2004) describes how he and his friends hacked programs and distributed them for free during their childhood: "It was like our donation to society, it was a form of honor; [we were] like Robin Hood bringing programs to people." Likewise, it is argued that culture and ethical attitudes may be a more crucial factor in driving software piracy as well as a number of other cybercrimes than the levels of economic development (Donaldson, 1996; Kshetri, 2009b, 2013a, b, c, d; Kwong et al., 2003).

Keywords: cyber-threats | cross-cultural management | cybercrime | culture

Chapter:

Introduction

As is the case of any economic activity, cultural factors are tightly linked to cybercrimes, cyber-attacks and cybersecurity. Just like any other activities, some forms of cybercrime may be more acceptable in some cultures than in others. For some categories of cyberoffenses, cultural factors appear to play more important roles than other environmental factors. For instance, cybercrimes are more justifiable in some cultures. Quoting a Russian hacker-turned-teacher, Blau (2004) describes how he and his friends hacked programs and distributed them for free during their childhood: "It was like our donation to society, it was a form of honor; [we were] like Robin Hood bringing programs to people." Likewise, it is argued that culture and ethical attitudes may be a more crucial factor in driving software piracy as well as a number of other cybercrimes than the levels of economic development (Donaldson, 1996; Kshetri, 2009b, 2013a, b, c, d; Kwong et al., 2003).

Theoretical, empirical and anecdotal evidence suggests that cultural factors exert a strong influence on the nature and patterns of cybercrime and cybersecurity. At the most basic level, cultural factors influence how issues around a crime (e.g., cybercrime) are constructed and how a cybercrime is defined (Brownstein, 2000). Unsurprisingly, the definition of cybercrime varies dramatically across cultures. Hamadoun Touré, secretary-general of the International Telecommunications Union (ITU) noted: "Pornography in one country is a crime; in another it's freedom of behavior" (Meyer, 2010). As such, cybercrimes and cyberoffenses have varying degrees of social and cultural acceptability across the world. They range from passive acceptance to outright celebration of "patriotic" hacker-heroes (Kshetri 2013d; Fowler, 2013). Indeed, important cross-cultural variation exists regarding what behavior is considered to be acceptable or unacceptable.

The orientation of a culture towards a cybercrime activity may differ depending on who the cybercriminals, victims and potential beneficiaries are. In the above example, distributing software stolen from a foreign company's website in a society may be received favorably because individuals in the society benefit from such activities. No less important in this example is who the victim is. The society may view a cybercrime differently when the victim is a foreign company rather than a domestic company. The idea of cultural Others may help us understand this phenomenon better. Jandt and Tanno (2001, p. 122) note: "In contemporary times as in colonial times, cultural Others have not been defined according to who they are but rather who they are not." In the same vein, Hoare (1991) argues that "all humans may possess the seeds of pseudo-speciation, of prejudice against dissimilar groups and values" (p. 52).

Due primarily to the newness of cybercrime, there has been surprisingly little theoretical and empirical work on the effects of cultural factors on cybercrime and cybersecurity. In general cyberspace the issue is underexplored in cross-cultural management (CCM). In an attempt to contribute to filling this void, in this chapter we seek to provide a better understanding of the link between cultural factors and cybercrime/cybersecurity and shed light on implications for CCM. In this chapter we try to achieve three objectives: (1) to explain how different aspects of culture are linked with definition and conceptualization of cybercrime, propensity to commit cybercrimes and types of cybercrimes likely to be committed; (2) to examine some elements of culture that are linked with cybersecurity; and (3) to illustrate how cyberattacks are more justifiable and acceptable from the perpetrator's point of view when the victims are cultural Others.

A cybercrime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules or regulations (Kshetri, 2009a). We follow the ITU's definition of cybersecurity:

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity

> strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. (ITU, U.D.)

Following Jandt and Tanno (2001), we use the term cultural Others to refer to "groups of people perceived to be outside defined boundaries, at the margins of acceptance" (p. 119).

Cultural factors affecting cybercrime

Prior literature has provided some indications on the link of culture with cybercrimes and cyber-security (Kshetri, 2005, 2006, 2009a; 2010a, b, c, d; 2013a, b, c, d; 2014a, b). Culturally supported habits influence the behaviors of relevant actors such as governments, firms, victims and hackers. As mentioned earlier, cultural factors influence how issues around a cybercrime are constructed, and how a cybercrime is defined, conceptualized, theorized, measured, responded to and policed (Brownstein, 2000). Saney (1986, p. 10) noted that culture is related to crime

> in its influence in encouraging certain types of antisocial behavior, in how we treat convicted felons, and in promoting the types of attitudes and perceptions in the public that either directly or indirectly influence the spread or restriction of criminal behavior in society.

Put simply, a crime is an activity or a behavior prohibited by a society, which falls within the society's criminal code (Cohen, 1992). As noted earlier, while pornography is crime in some countries, it is not in others. The Arab culture offers an interesting setting to illustrate this idea. Cultural, socio-political and cognitive factors in the region have important effects on these economies' cybercrime fighting measures. In August 2010, Saudi Arabia's Commission for the Promotion of Virtue and Prevention of Vice (also known as the Haia) announced that it would establish a unit to fight cybercrimes. The Haia also noted that the cybercrime unit's initial focus would be on cases involving online blackmail of women (arabianbusiness.com, 2010).

Some cultural factors provide a conducive environment for cybercrime activities. For instance, Husted (2000) found evidence that software piracy is more likely to occur in a culture that puts emphasis on sharing among group members, suggesting that a possible solution for piracy in this culture is to demonstrate piracy as a shameful act. Evidence also shows that most high-profile and widely publicized cybercrimes in India are concentrated in the offshore sector. It was reported in February 2010 that an employee in the IT giant Wipro used his colleague's password to steal some U.S.$4 million from the company's bank account (Mishra, 2010).

Culture's effect on the nature of cybercrimes committed by cybercriminals

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

As is the case of crime subculture observed in the conventional world (De La Calle Robles, 2007), what seems to be happening is region-specific specialization in cybercrime activities. Evidence indicates that cybercrimes originated in Asia exploit vulnerabilities in common software applications to steal personal information. Eastern European criminals are linked with organized crimes and identity theft (Fitzgerald, 2008). Romanian criminals, for instance, have distinctive advantage in online auction frauds. In auctions for big-ticket items, Romanians arguably "own the game" (Wylie, 2007). They have allegedly developed an ecosystem to auction fraud bringing together various players and technologies. Likewise, the Ukrainian criminal world is considered to be a "leader" in online credit card crime (Wylie, 2007). Hackers from the Middle East, on the other hand, have a higher tendency to deface websites (Fitzgerald, 2008). Likewise, Skorodumova (2004) linked national subculture with different characteristics of intrinsically motivated hacking.

Some cyberspace activities that are considered as cyberoffenses in some contexts are more likely to be justified in other cultural contexts. For instance, a *Business Week* article (23 June 2008) reported that China's public relations firms such as Daqi.com, Chinese Web Union and CIC charge U.S.$500–$25,000 monthly to monitor online posts. They help minimize the impact of negative information and create positive brand value for the company. There are reports that these PR firms hire students to write good posts about certain brands and to criticize the competition. While critics are concerned about the manipulation of consumer reviews and paid reviews, astroturfers in China have not faced legal problems. Note that in an astroturfing activity, the sponsoring organization of a message is masked, which is common in China outside of cybercrime as well. One way to understand the China–U.S. difference is to consider their experiences with modern capitalism. Many successful firms in mature market economies are guided by customer orientation and demonstrate their commitment to customer focus. Customers in these economies exhibit a low tolerance for poor behavior if businesses and suppliers do not fulfill their implicit and explicit commitments. Due to China's short history of modern capitalism, Chinese clients and customers are more likely to tolerate an absence of business ethics and a low level of product and service quality and/or reliability (Kshetri, 2010a, 2011).

Culture and cybersecurity

Our discussion thus far has focused on how various aspects of culture are linked to cybercrime. However, there is also another side of the coin, namely, cybersecurity. While the top security software firms are U.S.-based, businesses and consumers in some developing countries (e.g., Southeast Asia) prefer to buy domestically manufactured software for reasons of nationalism (Information Today, 2008; Kshetri, 2010c). Prior research has also suggested that cultural factors are linked to national development of cybersecurity skills. A senior fellow at Tokyo's Center for International Public Policy Studies notes that, in common with other professionals, Japanese cybersecurity specialists seek lifetime employment. In highly mobile job markets such as in the U.S., however, workers frequently move among the public sector, private sector and academia, which facilitates the institutional transfer of IT skills (Kshetri, 2014a). The lack of job mobility has led to a severe shortage of cybersecurity skills in Japan. As reported in a Reuter's article on 17 March 2014, Japan's IT minister, Ichita Yamamoto, admitted that the country's cybersecurity is lagging behind the U.S. and emphasized promoting computer science programs among

Japanese students in order to reduce reliance on imported security software and strengthen cybersecurity.

Let's take another example to illustrate the effect of culture on cybersecurity. Indian firms engaged in outsourcing have taken measures to prevent cybercrimes by current and former employees. Indian and foreign firms are following the security practices of Western firms, some of which are incompatible with local culture. For instance, call center employees have to undergo security checks, which are considered to be "undignified" (*The Economist*, 2005). The U.S. computer firm Dell faced difficulties in retaining its employees in its Indian call centers when the company attempted to emulate its headquarters model in treating the local employees (Kaka, 2006).

Justifiability and acceptability of victimizing cultural Others

Some examples of boundaries that separate perpetrators and potential victims and are likely to make cyberattacks more justifiable and acceptable from the perpetrators' perspective are presented in Table 30.1.

Table 30.1 Some examples of boundaries that separate perpetrators and potential victims and make cyberattacks more justifiable and acceptable

Source of otherness	Explanation	Some examples
Different nationality	Launching cyberattacks against individuals and organizations from other nations	Chinese hackers' cyber wars with Indonesians, Japanese and U.S. hackers
Different ideology	Using cyberattacks as a tool to attack an ideology	A Japanese student attacking Korean Internet servers to protest the war in Iraq
Different religion	Using cyberattacks against those who challenge one's religious beliefs and values	India-Pakistan and Israel-Palestine cyber wars
Economically more privileged classes	Launching financially motivated cyberattacks against rich people	Indonesian hackers targeting rich Westerners

Different nationality

Nationalism and patriotism are universally accepted as vital elements of state strength (Alagappa, 1995, 26–27). Salmon (1995) argues that "patriotism or attachment to one's country often leads to actions and attitudes which are disinterested or self-sacrificing, help solve free-riding problems" (p. 296). Prior research has shown that patriotism and nationalism provide cognitive legitimacy of some hackers' activities. We can find many instances of hackings linked to nationalism and patriotism. To take an example, in the early 1990s, a group of Portuguese hackers named TOXYN infiltrated a number of Indonesian government websites to fight against the occupation of East Timor (de Kloet, 2002). Indonesian hackers responded by attacking Portuguese servers that hosted the East Timor movement (Antariksa, 2001). To take another example, in 1997, cyberattacks occurred in Sri Lanka in support of the Tamil Tiger separatists. The strike was intended to disrupt government communications by overloading Sri Lankan embassies with millions of emails (Havely, 2000). To take yet another example, in 1998, the Indian army's website on Kashmir was hijacked by supporters of Pakistan's claim to the disputed territory, who plastered the site with their own political slogans (Havely, 2000). In response, in July 2001, the website of the Pakistan-based militant outfit Lashkar-e-Tayiba was attacked by a

hacker who called himself/ herself "True Indian" (Peer, 2001). It was in response to attacks of G-force, a Pakistani hacker group, to the Indian Ministry of External Affairs' websites.

We further illustrate this idea with examples of Chinese hackers' engagement in cyber wars, especially with U.S. hackers. Before proceeding further, let us briefly review Chinese and U.S. versions of nationalism and patriotism. Pei (2003) has identified several dimensions of nationalism. Consider two of them: source and bases. In terms of source, he argues that some examples of nationalism are a product of grass-root voluntarism (as U.S. nationalism) while others are fostered by government elites and promoted by the apparatus of the state (police, military, state-run media). Chinese nationalism is viewed as state sponsored and an attempt to fill an "ideological vacuum" left by the weakening socialism (Christensen, 1996; Oksenberg, 1987). In terms of bases, Pei distinguishes nationalism related to universalistic ideals (democracy, rule of law, free marketplace) and institutions from that based on ethnicity, religion, language and geography. China falls into the latter category. In China, the state arguably bolsters its legitimacy through invoking a deep sense of "Chineseness" among citizens (Ong, 1997; Barme, 1999; Hansen, 1999). China has adapted a body of complex scholarship to invoke a deep sense of "Chineseness." Sautman (2001) concludes: "Nowhere is this more pronounced than in China, where these disciplines [archaeology and paleoanthropology] provide the conceptual warp and woof of China's racial nationalism."

Chinese hackers have expressed their patriotic and nationalistic longings in several cyber wars. In August 1999, Web defacements led to a cyber war between Chinese and Taiwanese hackers. Initially, Chinese hackers defaced several Taiwanese websites with pro-China messages and said that Taiwan was and would always be a part of China (Denning, 2001). The Chinese have also fought cyber wars with Indonesians and Japanese hackers (de Kloet, 2002).

The U.S.–China cyber wars are particularly telling. In September 1999, following the accidental bombing of the Chinese Embassy in Belgrade, a group of hackers that identified itself as Level Seven Crew, defaced the website of the U.S. embassy in China and replaced the home page with racist and antigovernment slogans (Denning, 2001). Following the collision of a U.S. surveillance plane and a Chinese fighter in 2001, a Chinese hacking group published its plans for a "Net War," which was planned to continue until the anniversary of the bombing in Belgrade. In response, hacking groups from the U.S., Brazil and Europe attacked Chinese websites. Chinese hackers reportedly attacked about 1,100 U.S. websites while U.S. hackers broke into 1,600 Chinese websites (Kshetri, 2005). Similarly, after the collision of a Chinese fighter jet with a U.S. surveillance plane in April 2001, a Chinese hacking group attacked hundreds of U.S. websites including that of the White House (Bridis, 2001).

A comparative study between mailings of Chinese and Americans indicated that fierce feelings of nationalist fervor had fueled both camps (Kluver, 2001, p. 7). On several American websites, Chinese left: "We are ready to devote anything to our motherland, including our lives" (Smith, 2001). The Chinese hackers involved in the attacks argued that they were patriotic and thus did not do anything wrong. Analyzing the U.S.–China cyber wars, Kluver (2001, p. 8) concluded that "the technological optimism which sees in the Internet the end of nationalism and parochialism is an unrealistic understanding of how the Internet functions as a medium for human interaction."

Different ideology

In addition to nationalism and religion, hackers' interests are also framed by ideologies such as fight against global capitalism and against nuclear proliferation (de Kloet, 2002). For instance, some hackers are likely to attack networks of big multinationals to fight against capitalism. To take an example of ideological hacking, in June 1998, six hackers from the U.S., the UK, the Netherlands and New Zealand (identifying themselves as Milworm) hacked the website of India's Bhabha Atomic Research Center (BARC) and left a message: "If a nuclear war does start, you will be the first to scream" (Denning, 2001). Similarly, in South Korea, 58 Internet servers were attacked by a Japanese student in November 2003 to protest the war in Iraq (Duk-kun, 2003).

Different religion

Hackings by Islamic activists are interesting examples of cyberattacks that fall in this category. Except for occasional India–Pakistan and Israel–Palestine cyber wars, hacking by Islamist activists was insignificant before 11 September 2001. mi2g Intelligence Unit reported increasing Islamist hacking, the targets being networks of the U.S., Britain, Australia and other coalition partners as well as domestic networks of Russia, Turkey, Indonesia, Pakistan, Saudi Arabia, Morocco and Kuwait.

The holistic nature of Islamic society could help explain why a high proportion of cyber-attacks originating from the Middle East and North Africa (MENA) region are motivated by religious factors. For instance, following the Israel Defense Forces' (IDF) interception of a flotilla carrying humanitarian aid to Gaza in May 2010, tens of thousands of email addresses, passwords and personal details of Israelis were allegedly stolen by Turkish hackers. It was reported that there was dispute among the Turkish hackers in the online forum about the appropriateness of using the information for financial gain. Some hackers felt that using the information to steal money would undermine their political agenda. There was also a discussion of what the Koran says is permissible to do with the money of "infidels" (haaretz.com, 2010).

Economically more privileged classes

Cultural attitudes towards the potential victim are also related to the perpetrators' propensity to engage in cybercrimes. It is, for instance, reported that many Indonesian hackers feel that cyber fraud is wrong but acceptable, especially if the credit card owner is rich and not an Indonesian. A carder reportedly said: "Yes, it's wrong but it really only hurts other rich countries that were dumb enough to let us. Why should an Indonesian get arrested for damaging American business?" (Shubert, 2003). Another carder said: "I only choose those people who are truly rich. I'm not comfortable using the money of poor people. I also don't want to use credit cards belonging to Indonesians. Those are a carder's ethics" (Antariksa, 2001, p. 16).

Discussion and implications

The previous discussion indicates that there are important cross-cultural dimensions of cybercrime and cybersecurity, which are more complicated than meets the eye. There are important cross-cultural differences regarding what actions or activities are viewed as cybercrimes and how such crimes are policed, enforced and disciplined. Important cross-cultural variations also exist in social orientation towards various ingredients of cybercrime, propensity to engage in cybercrimes, attitude towards potential victims and nature of cyberoffenses committed. Finally, this chapter has provided a new perspective on the literature of the cultural Other by providing an overview of boundaries separating perpetrators and potential victims, which are likely to make cyberattacks more justifiable and acceptable from the perpetrators' perspectives.

Prior researchers noted that compared to formal rules, which may change quickly due to political and judicial measures, deliberate policies and actions often would have little effect to change informal institutions such as cultures and norms (North, 1990). Basic international patterns of cybercrimes and cyberattacks are less likely to change significantly in the near future. That is, one can expect cyberattacks driven by nationalism during international conflicts and wars from China. Hackers from the MENA region are likely to engage mostly in politically and ideologically motivated cyberattacks. Cybercrimes from Eastern European economies, on the other hand, are likely to involve economic gains.

Likewise, cybercriminals' cultural attitudes towards the potential victims of various categories are less likely to change in the near future.

That does not imply, however, that cultures related to cybercrime and cybersecurity cannot be changed at all. Since cultural factors affect the attitudes of individuals and organizations towards cybercrime and cybersecurity capabilities across countries, policy makers can make efforts to influence culture so that it is more intolerant of cybercrimes and conducive to cybersecurity. Perhaps an initial step is building a cybercrime consciousness, and a common understanding about the economic and social costs of cybercrimes and cybersecurity among citizens in order to prompt new habits of cybercrime avoidance and protection.

While this chapter has focused on cultural factors, these factors are not, in themselves, sufficient to explain cybercrime and cybersecurity. Further studies are warranted to fully understand the patterns of cybercrime cases and measures for cybersecurity across countries. These studies would undoubtedly contribute to creating a secure cyber environment for businesses and consumers.

The insights developed in this paper have important implications for CCM. The most often cited figure for the annual worldwide loss to cybercrime is U.S.$1 trillion and according to the 2011 Norton Cybercrime Report released by Symantec, 69 percent of the world's Internet users have been victimized by cybercriminals at some point in their lives (Kshetri, 2013d). The impact of cultural factors on cybercrime and cybersecurity as noted here suggests that the standard recipes, models and procedures for firms to be culturally aware and sensitive are highly inadequate for engagement with international crime of this complexity and on this scale. A related point is that whereas companies have faced rapidly growing cyber threats, a one-size-fits-all approach cannot address the global cybersecurity challenges. The degrees and types of threats faced by a multinational company are likely to differ drastically across countries. The discussion suggests

that different cultures differ in the degree to which various forms of intrinsically and extrinsically motivated hacking activities are committed by individuals. Likewise, cybersecurity-related training to employees, and other interventions are more important in some cultures. For instance, an emphasis on the importance of keeping one's password confidential might be necessary in cultures that view sharing among group members as an important social aspect.

This chapter also makes it clear that a firm that is characterized by a high degree of Otherness in a foreign country is more likely to face cyberattacks. For instance, a multinational company is more likely to be a cybercrime victim in a country characterized by resistance to capitalism. Likewise, a Western company is more likely to be associated with economically more privileged classes in a country where the majority of the population is poor, and is thus likely to face cyberattacks.

References

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

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

arabianbusiness.com . (2010). Saudi Arabia's Hai'a to set up cybercrime unit. Retrieved from http://www.arabianbusiness.com/saudi-arabia-s-hai-a-set-up-cyber-crime-unit-342746.html(accessed 26 May 2011).

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

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

Brownstein, H. H. (2000). The social production of crime statistics, Justice Research and Policy, 2, 73–89.

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

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

Cohen, M. A. (1992). Environmental crime and punishment: Legal/economic theory and empirical evidence on enforcement of federal environmental statutes. Journal of Criminal Law and Criminology, 82, 1054–1108.

de Kloet, J. (2002). Digitisation and its Asian discontents: The internet, politics and hacking in China and Indonesia. First Monday, 7(9). http://firstmonday.org/issues/issue7_9/kloet/index.html. Accessed 5 October 2006.

De La Calle Robles, L. (2007). Fighting for local control: Street violence in the basque country. International Studies Quarterly, 51(2), 431–455.

Denning, D. E. (2001). Chapter eight: Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In J. Arquilla and 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).

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

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

Fitzgerald, P. (2008). Crash of civilizations. Foreign Policy, September/October, 122.

Fowler, T. (2013). Book review: Cybercrime and cybersecurity in the global south, telecommunications policy http://dx.doi.org/10.1016/j.telpol.2013.11.004

haaretz.com (2010). Turkish hackers steal personal details of tens of thousands of Israelis. http://www.haaretz.com/news/diplomacy-defense/turkish-hackers-steal-personal-details-of-tens-of-thousands-of-israelis-1.302494 (accessed 29 May 2011).

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

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

Hoare, Carol H. (1991). Psychosocial identity development and cultural others. Journal of Counseling & Development, 70(1), 45–53.

Husted, B. W. (2000). The impact of national culture on software piracy. Journal of Business Ethics, 26(3), 197–211.

Information Today (2008). Challenges in the East. 25(2), 22

ITU (U.D.). Definition of cybersecurity, International Telecommunications Union (ITU) http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (accessed 29 May 2011).

Jandt, Fred E. & Tanno, Dolores V. Howard (2001). Decoding domination, encoding self-determination: intercultural communication research processes. Journal of Communications, 12(3), 119–135.

Kaka, N. F. (2006). Running a customer service center in India: An interview with the head of operations for Dell India, Mckinsey Quarterly, Web exclusive, May, http://www.mckinseyquarterly.com/article_page.aspx?ar=1779andL2=13andL3=13andsrid=17andgp=0 (accessed 2 May 2007).

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

Kshetri, Nir (2005). Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 11(4), 541–562.

Kshetri, Nir (2006). The simple economics of cybercrimes. IEEE Security and Privacy, January/February, 4 (1), 33–39.

Kshetri, Nir (2009a). Positive externality, increasing returns and the rise in cybercrimes. Communications of the ACM, 52(12), 141–144.

Kshetri, Nir (2009b). Institutionalization of intellectual property rights in China. European Management Journal, 27(3), 155–164

Kshetri, Nir (2010a). The economics of click fraud. IEEE Security & Privacy, 8(3), 45–53.

Kshetri, Nir (2010b). The global cyber-crime industry: Economic, institutional and strategic perspectives. New York, Berlin and Heidelberg: Springer-Verlag.

Kshetri, Nir (2010c). Diffusion and effects of cybercrime in developing economies. Third World Quarterly, 31(7), 1057–1079.

Kshetri, Nir (2010d). Cloud computing in developing economies. IEEE Computer, 43(10), 47–55.

Kshetri, Nir (2011). Privacy and security aspects of social media: Institutional and technological environment. The Pacific Asia Journal of the Association for Information Systems, 3(4), 1–20.

Kshetri, Nir (2013a). Cyber-victimization and cybersecurity in China. Communications of the ACM, 56(4), 35–37.

Kshetri, Nir (2013b). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4–5), 372–386.

Kshetri, Nir (2013c). Cybercrime and cyber-security issues associated with China: Some economic and institutional considerations. Electronic Commerce Research, 13(1), 41–69.

Kshetri, Nir (2013d). Cybercrime and cybersecurity in the global south. Basingstoke: Palgrave Macmillan.

Kshetri, Nir (2014a). Japan's changing cybersecurity landscape, IEEE Computer, 47(1), 83–86.

Kshetri, Nir (2014b). China's data privacy regulations: A tricky trade-off between ICT's productive utilization and cyber-control. IEEE Security & Privacy, 12(4), 38–45.

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

Meyer, D. (2010). ITU head: Cyberwar could be 'worse than tsunami', 3 September, ZDNet, www.zdnet.com/itu-head-cyberwar-could-be-worse-than-tsunami-30400.

Mishra, B. R. (2010) 'Wipro unlikely to take fraud accused to court', business-standard.com , 19 February, at http://www.business-standard.com/india/news/wipro-unlikely-to-take-fraud-accused-to-court/386181/ (accessed 29 May 2011).

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

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

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

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

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

Salmon, P. (1995). Nations competing against themselves: An interpretation of European integration. In A. Breton , G. Galeotti , P. Salmon , and R. Wintrobe (Eds.), Nationalism and rationality. Cambridge: Cambridge University Press.

Saney, P. (1986). Crime and culture in America. Westport, Connecticut: Greenwood Press.

Sautman, B. (2001). Peking man and the politics of paleoanthropological nationalism in China. The Journal of Asian Studies, 60(1), 95–124.

Shubert, A. (2003, 6 February). Taking a swipe at cyber card fraud. CNN.com . http://www.cnn.com/2003/WORLD/asiapcf/southeast/02/06/indonesia.fraud (accessed 27 October 2006).

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

Smith, C. S. (2001, 13 May). The first world hacker war. New York Times, 4.2.

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

Wylie, I. (2007, December 26). Internet; Romania home base for EBay scammers; The auction website has dispatched its own cyber-sleuth to help police crack fraud rings. Los Angeles Times, C.1.