Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations

By: Nir Kshetri

Kshetri, Nir (2013). “Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations" *Electronic Commerce Research* 13 (1): 41-69.

The original publication is available at:
http://link.springer.com/article/10.1007%2Fs10660-013-9105-4

Abstract:

China is linked to cybercrimes of diverse types, scales, motivations and objectives. The Chinese cyberspace thus provides an interesting setting for the study of cybercrimes. In this paper, we first develop typology, classification and characterization of cybercrimes associated with China, which would help us understand modus operandi, structures, profiles and personal characteristics of cybercrime organizations and potential perpetrators, the signature aspects and goals of cybercrimes, the nature and backgrounds of the criminal groups involved, characteristics of potential targets for criminal activities, the nature and extent of the damage inflicted on the victims and the implications to and responses elicited from various actors. We then examine this issue from developmental and international political economy angles. Specifically, we delineate salient features of China’s politics, culture, human capital and technological issues from the standpoint of cyber-security and analyze emerging international relations and international trade issues associated with this phenomenon. Our analysis indicates that China’s global ambition, the shift in the base of regime legitimacy from MarxLeninism to economic growth, the strong state and weak civil society explain the distinctive pattern of the country’s cyber-attack and cyber-security landscapes.

Keywords:

China | cybercrime | cyber-security | international relations | international trade | cyber security alliances | electronic commerce

Article:

1 Introduction

While researchers are beginning to address the issues related to the dark side of e-commerce such as security breach and other forms of cyber-attacks [1, 2], sufficient attention has not been given to this topic. For various reasons, China provides an ideal laboratory to study, observe, document and understand this phenomenon, especially diverse aspects of cybercrimes including the associated contexts, mechanisms and processes. These factors are tightly linked with various key concepts related to e-commerce such as web trustworthiness, information control and privacy, which affects users' perception of e-commerce providers as well as the broad environment [3–5].

Prior research indicates that cybercrime and cyber-security in developing economies have unique structural characteristics [6, 7]. Yet the literature does not discuss how key economic, political and social characteristics of developing countries such as low levels of human development and education and weak democratic institutions [8] are connected to cybercrime and cyber-security.

Cybercrime and cyber-security issues have increasingly important international dimensions. With the decline of violent geopolitical conflicts, traditional issues such as nuclear war are losing their salience and importance and the focus and organizing principle in international relations have been on nontraditional security issues including cyber-security [9–15]. Cyber-security is thus becoming one of the biggest "hot button" issues in international relations and international politics.

Prior research has also suggested that countries' military alliance is positively related to trade relations [16]. In recent years, a number of alliances have been formed according to cyber-security-related interests. These alliances have dramatic potential for bringing significant changes in international trade and investment relations among countries.

To put things in context, the complexity of China-originated cyber-attacks has discouraged foreign Internet firms to operate in the country. To take an example, in 2008, Google's CEO said that his company would work with Chinese universities, starting with Tsinghua University, on cloud computing-related academic programs. The cyber-security environment, however, led to Google's withdrawal from China. There are also important international relation dimensions of cyber-attacks originated from China. For instance, an FBI Assistant Director noted: "Cybercrime … is the fastest-growing problem faced by China-US cooperation" [17].

Scholars have not, however, explicitly investigated these issues. This article seeks to bridge the gap in understanding about the role of cyber-security in international relations, international politics and related areas. Against the backdrop of the above observations, it attempts to unravel the complexities and mechanisms involved in this new war, reconfiguration of the existing organized crime groups, emergence of the new international organized crime groups, and the changing nature of the constraints facing the states.

This paper seeks to fill this gap. Specifically, this paper has two objectives. The first is to discuss the typology of cybercrimes originating from and/or affecting China. The second objective is to

analyze the developmental and international dimensions of cybercrime and cyber-security issues associated with China.

The paper is structured as follows. We proceed by first providing a brief survey and developing a typology of cybercrimes and applying in the context of the Chinese cyberspace. Next, we develop a framework that links developmental and international dimensions with cybercrime and cyber-security. Then, we apply the framework in the contexts of cybercrime and cyber-security in China. It is followed by a section on discussion and implications. The final section provides concluding comments.

2 A survey and typology of cybercrimes in China

A report of the China Internet Network Information Center indicated that, in the first half of 2011, 217 million Chinese (45 % of the country's Internet population) became victims of virus or Trojan horse attacks, 121 million had their online accounts hacked or passwords stolen, and 8 % were victimized by online scammers [18]. Gao Xinmin, a vice president of the government-backed Internet Society of China (ISC) noted that China's infrastructures as well as information systems of major organizations and industries have become cyber-attack targets [19]. Likewise, speaking at the Fourth US-China Internet Industry Forum in November 2010, Gu Jian, a vice-director of the Ministry of Public Security 's network security protection bureau, noted that 80 % of computers connected with the Internet in China had been controlled by botnets at some point [20]. Many cyber-attacks target China for the simple fact that the country is rapidly digitizing and integrated with the global economy. For instance, Chinese consumers also suffered when the stockbroking service E*Trade experienced a distributed denial of service attack in December 2011.

Table 1 presents some representative studies on China's position in the global cyber-attack industry. A report from NetQin Mobile in August 2011 indicated that China accounted for 64 % of mobile Android attacks. The shares of the US and Russia were 7.6 % and 6.1 % respectively. In general, most versions of the premium rate "dialer" Trojans are downloaded through app stores in China and Eastern Europe. China is also among the top click fraud originating countries outside North America (Table 1).

Table 1

Some representative studies on China's position in the global cyber-attack industry

Time	China's position in the global attack industry
First-half of 2002	China ranked 4th in total cyber-attacks (6.9 %)[a]
2006	Symantec report: 5 % of the world's malware-infected computers were in Beijing. China overtook the US in the number of malware hosts
2006	An annual survey of CyberSource Corp. ranked China as the world's second riskiest country for online transactions, only behind Nigeria[b]
2006Q1	China was the top click fraud originating country outside North America (tied with France)[c]
2007	China hosted more malware than any other countries (51.4 %)[d]
2007	China ranked second in the list of top infection program creating countries (30 %)[e]
Second-half of 2007	China ranked second in the list of top countries hosting phishing websites (14 %)[f]
Second-half of 2007	China ranked fourth in the list of top countries generating spam (4 %)[f]
2008Q1	China was the top click fraud originating country outside North America (4.3 %)[g]

[a] [*21*]; [b] [*22*]; [c] ClickForensics study; [d] sophos.com (2008); [e] [*23*]; [f] Symantec Internet Security Threat Report Vol. XIII, 2008; [g] Click fraud network study

It would be interesting to look at some indicators related to China's imports versus exports of cybercrimes. For one thing, the Chinese government commonly blames foreign hackers for cyber-attacks targeting the country. For instance, Gu Jian of Chinese Ministry of Public Security said that over 200 Chinese government websites experience cyber-attacks on a daily basis and most attacks are foreign-originated [20]. According to Information Office of the State Council, over one million IP addresses in China were controlled and 42,000 websites were hijacked by foreign hackers in 2009 [20]. Likewise, according to a report of China's Computer Emergency Response Team (CNCERT), the country's 8.9 million were attacked by 47,000 foreign IP

addresses in 2011 [24]. The report noted that foreign hackers compromised 1,116 Chinese websites in 2011.

Data proxies and indicators from a number of sources across a long time period indicate that substantial cyber-attacks originate in China. First, let us look at foreign and domestic origins of malware infecting Chinese computers. One such indicator concerns the malware infection rate per 1000 computers (MIR) based on the telemetry data collected by Microsoft from users of its security products opting in. The telemetry data indicated that China was among the countries with lowest infection rates (Fig. 1). Another measure is Sophos' threat exposure rate (TER), which measures the percentage of PCs experiencing malware attacks. China was the second most malware infected country only behind Chile in the third quarter (Q3) of 2011 with a TER of 45 (Fig. 2).

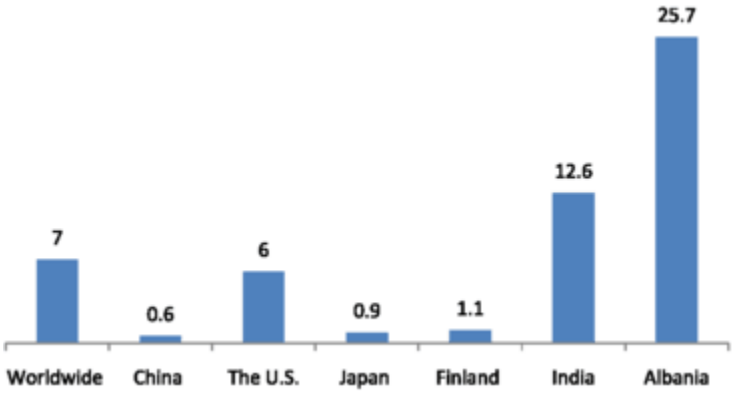

Fig. 1

A comparison of malware infection rates in China and selected other economies (2012, 2Q). Source: [25]. The number of reported computers cleaned for every 1,000 executions of the Microsoft Malicious Software Removal Tool (MSRT)

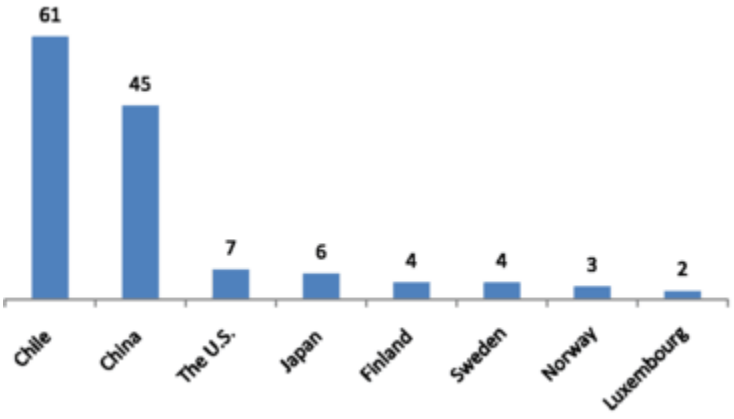

Fig. 2

A comparison of China's threat exposure rate (TER) with selected economies. Source: [26]

The explanation regarding the differences in the two studies is that they differ in ability to detect Chinese and foreign malware. While TER captures all types of malware, telemetry data only detect globally prevalent malware. A Microsoft report concluded that the low infection rate as detected by telemetry can be attributed to unique Chinese malware landscape that tends to be dominated by Chinese-language threats not found elsewhere [27]. This analysis is consistent with the views of security observers in Europe and the Americas, who say that they do not receive most of the Chinese-language phishing e-mails and instant messages [28].

It is important to triangulate this evidence with that coming from other sources. In 2005 and 2009, China ranked #2, behind the US, in top countries for originating cyber-attacks [29]. According to the Anti-Phishing Working Group (APWG), 70 % the world's maliciously registered domain names were established by the Chinese to attack domestic businesses. In 2011H1, Chinese perpetrators established 11,192 unique domain names and 3,629 .cc subdomains for such attacks, majority of which attacked Chinese companies and 80 % targeted Taobao.com. Likewise, according to APWG, China had the world's highest malware infection rate of 54.1 % in 2012Q1.

2.1 A typology of cybercrimes in China

It is important to recognize that cybercrimes originating from and affecting China are far more complicated than what is presented in Table 1 or what the popular press has characterized and described. We first develop a typology of cybercrimes as a starting point and apply it in the context of the Chinese cyberspace (Fig. 3). The typology would help us understand the extent, nature, causes and consequences of cybercrimes associated with China. This is important in light of the reports regarding a division of the labor across various activities associated with the Chinese cybercrime industry [30, 31].

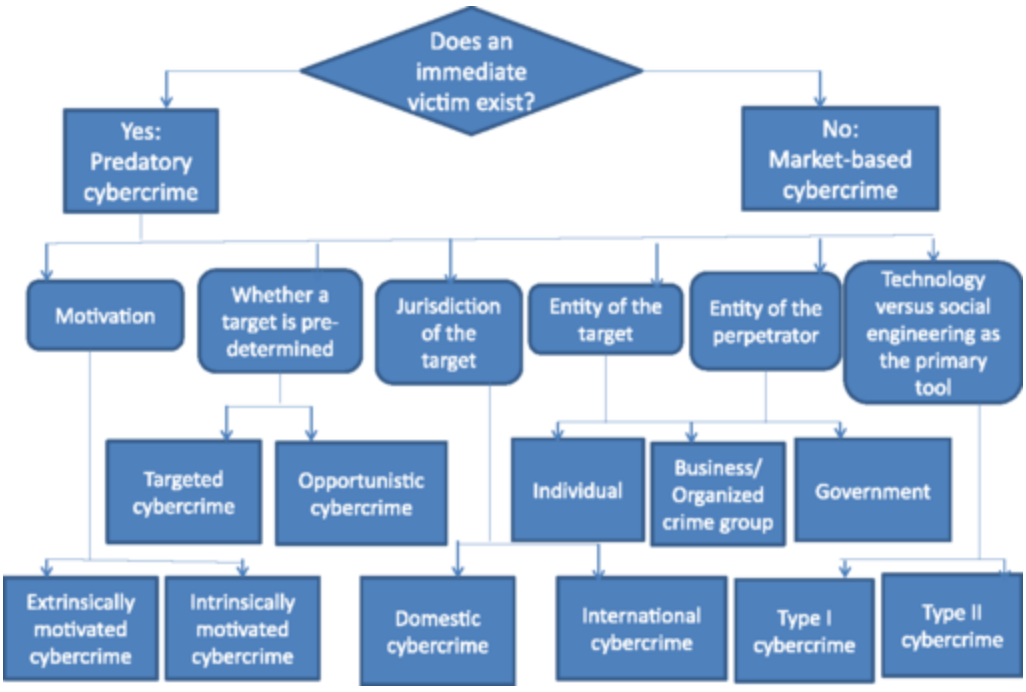

Fig. 3

A typology of illicit activities in the cyberspace

Such a typology would suggest how cybercrimes with certain characteristics and behaviors have a certain probability of targeting a given victim and what reactions and responses they are likely to receive from various actors. A typology would also have significant implications for consumers, businesses and governments in taking precautionary and defensive measures. For instance, cybercrimes associated with political and economic espionage can result in dramatically different responses and outcomes. The typology can also be used to explain the shifts in the cybercrime landscape. Furthermore, a typology would help adopt unified strategy to fight cybercrimes. In addition, such a typology would also provide a useful basis for further research on cybercrimes.

Predatory and market-based cybercrime

In a market-based cybercrime, goods and services are illegally produced and/or distributed online. There are instance of market-based cybercrimes associated with China. One example is China's export of cybercrime enabling technologies and equipment to international groups. For instance, crime rings involved in identity theft and credit-card-forgery in New York City allegedly sourced their skimming equipment, including blank credit cards from China, Lebanon, Libya, and Russia [32]. In this paper we mainly focus on predatory cybercrimes.

Combining the definitions of predatory crimes in the conventional setting (e.g., [33, 34]) and cybercrime [35], we define a predatory cybercrime as a crime in which an offender inflicts a

harm or takes property from a victim by using computers or computer networks are the principal means.

Motivations associated with cybercrimes

The first issue is to examine the motivations of cybercrimes associated with China. Curiously, there is a higher degree of prevalence of extrinsically motivated cybercrimes that are committed for external rewards or financial benefits. However, while Russia- and Eastern-Europe-based cybercriminals' activities tend to revolve around monetizing from malicious applications, proportionately more China-connected cybercriminals seem to be interested in gaining access to intellectual property (IP) and trade secrets. For instance, according to Symantec at least 29 firms in the chemicals industry were targeted by cyber-attacks traced to China in July–September 2011. Moreover, 19 companies including defense specialists were also affected [36]. Twelve of the companies were US-based, five in the UK, and two in Denmark.

There are many instances of insider cybercrimes in the West that have been allegedly linked to China. A 2011 report titled, "Foreign Spies Stealing US Economic Secrets in Cyberspace" published by the Office of the National Counterintelligence Executive suggested that some Chinese companies used ethnic Chinese "insiders" to steal information from Western companies. In 2005, a Chinese intern working in Valeo was detained in France for alleged database intrusion aimed at IP theft. In 2011, a Chinese-born scientist was convicted for stealing trade secrets from Cargill and engaging in economic espionage at Dow AgroSciences. Cargill estimated that the information stolen by the scientist was worth US$12 million in R&D [37]. Similarly, a Motorola employee arrested by US Customs in Chicago allegedly possessed a one-way ticket to China and proprietary information that was worth $600 million in about 1,000 electronic documents [38]. To take another example, an employee at Valspar Corporation, who was arrested in 2009, allegedly downloaded 160 formulas for paints and coatings, which were estimated to cost the company about $20 million in R&D or about one-eighth of the company's annual profits [39]. In a similar case, another chemist at DuPont downloaded data on organic light-emitting diodes, which he allegedly intended to transfer to Beijing University [39]. It was also reported that China-based hackers attacked DuPont's computer networks two or more times in 2009 and 2010 [40]. In the same vein, a product manager at Ford Motor Company allegedly made unauthorized digital copies of about 4,000 documents, which would help him to get a job with a Chinese automobile company [39].

Nonetheless, while online theft of financial credentials and bank accounts is the signature aspect of mainly cybercriminals from Russia and Eastern Europe, some of such frauds have been traced to China. According to the Federal Bureau of Investigation (FBI), between March 2010 and April 2011, there were 20 incidents in which cybercriminals initiated to transfer large sums from the accounts of US businesses to companies registered in cities near the China-Russia border. The criminals attempted to transfer about US20millionbutsucceededtotransferabout11 million. The attacks mainly involved botnets that are often used in banking frauds such as Zeus botnet,

Backdoor.bot or Spybot [41]. As soon as the transfers went through, the sums were withdrawn from or transferred out of the recipients' accounts.

There are also many instances of intrinsically motivated cybercrimes, which are committed for inherent satisfactions rather than an external reward or some separable consequence. Especially, obligation/community-based intrinsic motivations associated with China-based cybercrimes deserve mention. Behaviors of ideological hackers interested in political goals can be explained by obligation/community-based intrinsic motivations. Chinese hackers, for instance, have expressed patriotic and nationalistic longings in cyber-wars. They have fought cyber-wars with Taiwanese, Indonesians, Japanese, and US hackers.

Technology versus social engineering as the primary tool

In Gordon and Ford's [42] categorization, Type I cybercrime mostly contains technological elements while Type II cybercrimes have mainly human elements. A high proportion of cybercrimes originated from China which pursue foreign targets belong to the Type I. However, China-based cybercriminals have also used social engineering techniques to manipulate people into divulging confidential information to gain access to the systems. For instance, in a series of cyber-attacks, which were traced to China by Symantec, the target firms had received emails, which asked them to open an attachment. The emails claimed that the attachments were invitations from established business partners or security updates [36]. The 2009 China-originated attacks on Google, also dubbed as Operation Aurora, relied heavily on social engineering tools. The attackers had communicated with employees in US firms such as Google, Adobe and Microsoft for a long period to gain trust. The attackers then sent messages asking them to click on websites infected with malware [43].

Cybercrimes involving social engineering tools that target Chinese consumers are also growing rapidly. This can be attributed to the rapid rate of Internet and e-commerce development in China. For instance, China added 55.8 million new Internet users in 2011 [28]. These novice and inexperienced users tend to lack an understanding of the dangers of phishing and more likely to be duped by the phishers' tricks.

Jurisdiction of the targets associated with China-originated cybercrimes

The contemporary Western view is that China is among the biggest exporters of cybercrimes. In many ways, much of the current debate about China-originated cyber-attacks represents a cyber Cold War.

As noted earlier, China is increasingly recognized as a major source of economically motivated cyber-attacks, the US being the most popular target. For instance, in 2005, a Trojan horse code named Myfip was reportedly sending data from the networks of US-based companies to an Internet user in Tianjin, China. Myfip sent sensitive documents such as CAD/CAM files containing mechanical designs, electronic circuit board schematics, and layouts [44]. Likewise, a

2009 report of Google noted that the Aurora attacks on its computer systems were a part of a larger operation that infiltrated the infrastructures of at least 34 other large companies [45]. Other reports had indicated that the hackers had attacked networks of more than 100 companies [46].

Cyber-attacks originated from China are highly globalized with multiple operations across the world. Industrialized countries are not the only targets of China-originated international cyber-attacks; in fact, many developing countries have been reportedly victimized by Chinese hackers. In 2011, McAfee researchers published a report indicating that hackers operating from China stole information related to operations, financing and bidding from oil companies based in the US, Taiwan, Greece and Kazakhstan [47].

It is erroneous and misleading to conclude that China-based cybercriminals only target foreign consumers, businesses and governments. According to a phishing survey released by the Anti-Phishing Working Group (APWG) in November 2011, phishing attacks against Chinese e-commerce and banking sites increased by 44 % in the first half of 2011. Unlike most phishers, Chinese phishers prefer to register new domains instead of using hacked domains. A report by the APWG in April 2012 indicated that Taobao.com overtook PayPal to become the world's most frequent phishing in the second half (2H) of 2011 [28]. In the 2H 2011, Taobao.com experienced 18,508 phishing attacks, which was 22 % of all the phishing attacks worldwide and over twice as much as PayPal.

Opportunistic and targeted attacks

The next issue concerns the predetermination and intentional selection of targets. As is the case of the general trend in the global cybercrime industry, China-originated cybercrimes are believed to be more targeted, often tied to specific high value targets, individualized and customized. Analysts have noted that a large proportion of the most sophisticated cyber-attacks aimed at extracting high-value IP, also known as, advanced persistent threats (APTs) originate from China [48]. Note that APTs are characterized by a high degree of stealthiness. They employ sophisticated means to gain access into a network, stay hidden and undetected, and compromise data for an extended period of time. In order to escape observation and avoid notice, they act quietly, cautiously, and secretly.

Category of the targets and victims (individuals, businesses and governments)

A critical issue concerns who the targets and victims of the cyber-attacks are. There is a wave of cybercrimes targeting individual consumers. For instance, the Trojan horse known as Geinimi corrupted a number of legitimate Android games on Chinese download sites, and added infected devices to a mobile botnet. In the last week of December 2011 alone, personal details of over 45 million Chinese consumers were stolen in separate cyber-attacks [49]. Increased digitization of economic activities has increased the value of personal information, which has provided incentives for cybercriminals to steal such information. As another example in this category, in April 2012, Chinese authorities shut down 42 websites, which allegedly extorted money from

individuals threatening to disclose “negative information” about the victims using fake accredited journalists. They had operated under the false names of government agencies and public welfare institutions.

The China-originated APTs have targeted governments as well as corporations [48]. There are instances of activists’ engagement in intrinsically motivated cybercrimes for which Chinese businesses are the targets and victims. A case in point is the country’s biggest dairy operator China Mengniu Dairy. The company’s website, www.mengniu.com.cn was attacked in December 2011 after the company admitted that its milk products contained a cancer-causing substance [49].

Chinese businesses have also become victims of financially motivated cybercrimes. One example concerns click fraud schemes. The market research firm Analysys’ survey in China conducted in 2006 indicated that one-third of respondents believed they had been click fraud victims. Likewise, a study by China IntelliConsulting found that Baidu had a click fraud rate of 34 %, compared to Google’s 24 % [23]. As another example, the extortion involving fake journalists mentioned above also targeted many organizations.

As another example, a Business Week article (June 23, 2008) reported that China’s public relations firms such as Daqi.com, Chinese Web Union and CIC charge businesses US$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 [50].

Foreign originated financially motivated cybercrimes victimizing Chinese businesses also deserve mention. According China’s Computer Emergency Response Team (CNCERT), 95.8 % of phishing websites targeting Chinese domestic banks in 2011 were foreign originated [24].

Finally, in addition to individuals and businesses, Chinese government agencies have also been victimized. For instance, in October 2001, a hacker in China replaced a Chinese government website with pornographic contents [51].

Category of the perpetrator (individuals, organizations/organized crime groups and government agencies)

Many cyber-attacks (e.g., on Mengniu’s website) may well be the works of individual, non-organized cybercriminals. There are reports that traditional organized crime groups in China have employed hackers and diverted their efforts from traditional activities to cybercrime [7]. According to the National Police Agency of Japan, about 90 % of bank accounts in Japan that received fraudulently transferred money online were opened under Chinese names. The Agency suspected that Chinese organized crime groups were behind these frauds. Yet another example of an involvement of organized crime groups associated with China in cybercrime activities, in April 2012, Malaysian police arrested more than 200 cybercriminals from China and Taiwan

[52]. Some companies have also engaged in cyber-attacks on rival companies' networks. In 2009, a cyber-attack by a Chinese online gaming company to the servers of its rival companies led to an Internet outage in many cities in China [30].

Finally, the Chinese government agencies have also reportedly engaged in cyber-attacks targeting domestic businesses and consumers. For instance, there were reports that the Chinese government agencies sent viruses to attack websites that were banned [53].

2.2 Combining different dimensions of Fig. 3

The different dimensions can be combined to identify and categorize cybercrimes so that a crime in each cell (or quadrant) exhibits the characteristics of both dimensions. As an example, various categories of cybercrimes are plotted onto a 2×2 matrix (Fig. 4) that illustrates the location of the target or victim (domestic versus international) on the x-axis against the motivation (extrinsic versus intrinsic) on the y-axis.

Victims/target⇒ Motivation ⇓	Domestic	International
Extrinsic	[I] • Some domestic industries are attractive cybercrime targets (e.g., online gaming) • Chinese cybercriminals with a lack of organizational capability to internationalize may focus on the domestic market • Weak defense mechanisms of Chinese targets	[III] • Industrial and economic espionage activities • Cybercrimes involving data and credential stealing malware aimed at committing financial frauds
Intrinsic	[II] • Politically motivated attacks on Chinese companies networks (e.g., Activists' attack on Mengniu Dairy websites) • Cyber-attacks on Chinese government agencies' websites • Chinese government's attacks on non-complying domestic websites	[IV] • Political espionage activities • Chinese nationals' engagement in international cyber-wars

Fig. 4 A 2×2 matrix of China originated cyber-attacks representing jurisdiction of the target/victim and motivation

As illustrated in Fig. 4 and discussed above, while digitization of the Chinese economy has increased the opportunities for extrinsically motivated cybercrimes, some domestic industries such as online gaming are more attractive (cell I). As illustrated in cell II, intrinsically motivated cybercrimes pursuing domestic targets have various combinations of perpetrators and victims involving individuals, businesses and governments.

China-originated extrinsically motivated cybercrimes pursuing international targets are found to focus primarily on industrial and economic espionage activities involving IP and trade secret thefts. Nonetheless, cybercrimes characterized by quick monetization which involve data and credential stealing malware aimed at committing financial frauds are traced to China (cell III). Finally, intrinsically motivated China-originated cyber-attacks pursuing international targets seem to be associated with alleged political espionage activities as well as Chinese nationals' engagement in international cyber-wars (cell IV).

3 Developmental and international dimensions of cybercrime and cyber-security

To understand the above observations regarding various types of cybercrimes associated with China, we look at this issue from developmental and international political economy viewpoints.

3.1 Economic and social characteristics of a developing economy

Some of the key economic and social characteristics of a developing country include a dual economy, low levels of income and education, which lead to low levels of human development; high unemployment rates, high degrees of income inequality, and weak democratic institutions [8, 54]. Prior e-commerce researchers have linked these characteristics with innovations, intellectual protection rights and diffusion of information technology in developing economies [55]. In this paper, we would argue that these characteristics are tightly connected to the natures of cybercrime and cyber-security.

For instance, low levels of income and education lead to relative laggardness in developing world-based consumers' adoption of new technologies. To put things in context, many Internet users in the developing world are inexperienced and not technically savvy as a high proportion of them got their computers and connected to the Internet not long ago. A majority of them also lack English language skills. This later point is crucial due to the fact that most of the information, instructions, and other contents for security products are available in English language only. Many Internet users in economies in the developing world are unable to use IT security products developed in English language [6, 7].

Equally important in this context is a higher intergenerational differences in computer use. Parents in the developing world tend to lack knowledge, skills, resources and capability to

supervise and monitor their children's online activities due primarily to a lack of computer skills. They cannot thus ensure that their children are not engaging in undesirable activities or have not been victimized online [14, 15].

Countries with weak democratic institutions face additional problems. In some authoritarian regimes, cyber-security measures mainly focus on cyber-control activities. For instance, Chinese government agencies allegedly sent viruses to attack websites that were banned [53]. Likewise, the governments of Myanmar and Mauritania have allegedly hired botnet operators to attack their critics' websites with DoS attacks [56]. The government of Myanmar had reportedly built up an advanced cyberwarfare department within the police force, which, in the past, tracked its online critics and sent virus attached e-mails to exiled activists. In 2008, before the anniversary of the Saffron Revolution, at least three websites associated with Burmese exiles experienced DDoS attacks.

Finally a developing economy could be described as a dual economy. In its basic form, a dual economy is characterized as one that has a relatively developed urban industrialized sector and a rural sector [54]. The dual nature of the economy also means that in addition to variation between sectors of the economy, developing economies are characterized by an uneven development within a given sector [57]. Cybercrimes targeting developing economies exhibit a heavy concentration in well-developed industry sectors such as businesses in the online gaming industry in China, banking and financial sectors in Brazil and offshoring sector in India [6, 7].

3.2 Causes of prosperity and poverty

While there is a wide, vast and bewildering array of ideas that encompass economic development and its causes, we attempt to develop a perspective on cybercrime and cyber-security which revolves around what we see as the key issues. Based on a review of the literature, Acemoglu [58] and Acemoglu, Johnson, and Robinson [59] have identified fundamental and proximate causes of prosperity and poverty. Institutions, culture and geography have been identified as fundamental causes of prosperity [58, 59]. Moreover, institutional theorists consider culture as an informal institution [60]. Given that geography has a limited role in cyber-security, we focus on the roles of formal and informal institutions. The basic idea is simple: economically successful societies are characterized by 'good' economic and political institutions [61]. Some elements of institutions such as corruption, lack of accountability and weak law enforcement may create bottlenecks for development [62, 63]. To put things in context, many developing economies' capability to build cyber-security related institutions, while the states "hold some trump cards" "at the most basic level", for instance, with their power to define the activities that are illicit [64], many governments lack technological sophistication and are poorly equipped to fight the non-state criminal actors.

Likewise, culture is related to different sets of beliefs regarding how people behave, which have strong implications for development [65]. An example relevant to the present investigation may illustrate the situation. While traditional illicit activities are more likely to be viewed as deviant and carry a social stigma [64], this is not necessarily the case for cybercrime related activities. For instance, many criminal hackers based in the developing world see their cybercrime activities victimizing developed world-based consumers and businesses as morally acceptable and legitimate (e.g., [66]).

Among the proximate causes are physical capital differences, technology differences, human capital differences and functioning of markets [58]. In this paper, we focus on technology differences and human capital differences, which are the issues that matter most to cybercrime and cyber-security.

In a framework proposed by [63] for an analysis of institutional bottlenecks in developing economies, technology-related issues and factors are present at three levels: technological progress and dissemination (institutional outcomes), technology opportunity set (interaction and decision area), technology use, adoption and development (intermediate outcomes) [63]. In this section, we analyze these elements from the perspective of cyber-security.

In expanding their attack sources such as botnets, hackers find it attractive to focus on economies with less developed information-security infrastructures [29]. In this regard, as to the technological progress and dissemination, most developing countries are characterized by poor performance in cyber-security infrastructure. For one thing, they lack domestic anti-virus companies. At the same time, while the top security software firms are based in industrialized economies, businesses and consumers in some developing countries (e.g., Southeast Asia), mainly because of nationalism, prefer to buy domestically manufactured software. One way to understand the low level of technological progress is the lack of absorptive capacity, which means that many developing economies exhibit a low level of national capabilities in the assimilation of technologies and associated organizational practices [67, 68]. This can be attributed to their institutional and social arrangements [69]. As to the technology opportunity set, developing economies have a tendency to use low cost, but insecure technologies.

As to the human capital, a high proportion of Internet users in developing countries are getting computers and connecting them to the Internet for the first time. A majority of new Internet users also lack English language. While the developments of user-friendly software and interfaces have reduced the complexity and consumer learning requirements for computer and Internet use, such developments have not taken place in the development of security products. Most of the information, instructions, and other contents for security products are available in English language only [70]. Many Internet uses are unable to use IT security products developed in English language.

3.3 International dimensions of cybercrime and cyber-security issues

Cybercrime and cyber-security issues are occupying an important and increasingly strategic role in international relations as well as international trades and investments. International relations aspect of cyber-security is reflected in the formation of major international bodies and various treaties and bilateral, regional and international agreements. As of September 2012, 47 countries had ratified, accessed, or signed the Council of Europe Convention on Cybercrime (http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG). Likewise, the Shanghai Cooperation Organization (SCO), which has Kazakhstan, China, Kyrgyz Republic, Russia, Tajikistan and Uzbekistan as members, has taken significant steps toward cyber-security cooperation.

One way to understand the importance of cyber-security in international relations is to consider this issue in relation to traditional issues. A large body of literature indicates that with the decline of violent geopolitical conflicts, traditional issues such as nuclear war are losing their salience and importance and the focus and organizing principle in international relations have been on nontraditional security issues such as small arms smuggling, drug trafficking and transnational crime, environmental degradation, illegal migration and people smuggling, disaster relief, counterterrorism and counterpiracy [9–13]. Cyberthreat is a legitimate security issue because cyber-attacks present threats to national security for the simple fact that most of the critical infrastructures are connected to the Internet. This issue is also tightly linked to economic security of countries.

In terms of the roles in facilitating illicit transnational economic activities, Andreas [64] describes the Internet as “simply the latest—and not necessarily the most important—chapter in an old story”. Many analysts, however, have suggested that the Internet has potentially dramatic consequences in terms of stimulating illicit cross-border activities that are unmatched by any other previous technologies. For instance, Robert Rodriguez, Chairman of the Security Innovation Network and senior adviser to the Chertoff Group noted: “Our nation [the US] is going through the greatest transfer of wealth in the history of mankind. And it’s because of the increasing vulnerabilities within our systems” [71].

Prior research has suggested that countries’ military alliance is positively related to trade relations [16]. This is especially true for countries which belong to the same alliance in a bipolar system with two roughly equal actors or coalitions of actors that divide the world economies into two poles such as during the Cold War. In a system with two major opposing alliance groups, countries that are allies tend to trade more freely among themselves [72]. Trade-related behaviors are driven by possible security externalities which provided fundamental motivation for helping their allies and punishing their enemies [72]. Some economies such as China, Russia and the US are concerned about cyber-security externalities of trades and investments in high technology. In this regard, new and emerging alliances related to cyber security and cyberwarfare are likely to shape the development of international political and economic institutions.

4 Applying the framework in the contexts of cybercrime and cyber-security in China

4.1 The developmental dimension of cybercrime and cyber-security

In this section, we discuss developmental aspect of cybercrime and cyber-security in China. Before discussing the fundamental and proximate causes of prosperity/poverty, it is necessary to discuss cybercrime and cyber-security in China from the dual economy perspective.

Dual economy and cybercrime in China

While the Internet is not within the reach of the huge poor rural population, some economic sectors are highly digitized and are attractive cybercrime targets. Due to this attractiveness, a significant proportion of China-originated malware target Chinese victims.

Being a rapidly digitizing economy with over 538 million Internet users by July 2012, China has been an attractive cybercrime target. In the first quarter of 2011, China overtook the US as the world's largest PC market, after three decades of US dominance in the industry. According to China e-Business Research Center and CNZZ Data Center, China's e-commerce market reached $703 billion in 2010, 22 % higher than in 2009 [73]. Security analysts have observed that phishing and other forms of cybercrimes targeting China can be attributed to an explosion of e-commerce in the country [28].

Cybercrimes in developing economies exhibit a heavy concentration in specific industry sectors. In China, for instance, businesses in the online gaming industry and gamers have been attractive targets for hackers [74, 75]. These hackers steal gamers' passwords and login information (e.g., World of Warcraft) and sell virtual items such as gold coins, weapons and armor from the stolen accounts. The stolen virtual items and identities are auctioned online [23]. Experts say that an online gaming account in China can be sold for up to US1,000 compared to US5–10 for stolen credit card data [76]. Online games generated US$1.8 billion in 2007 [77], which increased to US$6.8 billion in 2011 [78]. Buying and selling of virtual items has been a "mini-economy" in China [79]. For instance, 11 members of a cybercrime ring, who were sentenced in 2009 made over $140,000 by selling stolen equipment and virtual currency [31].

In China's arguably largest reported cyber-fraud, law enforcement agencies arrested a gang, which allegedly stole $48 million from small businesses. The criminals contacted potential victims via the instant-messaging service QQ and offered naive users a link to a fake deal that looked attractive. Computers of users who clicked on the link were infected with malware, which stole online payment details such as login credential for PayPal. The criminals used the accounts to buy credits for online games and sold them for cash [80].

China also provides an example to illustrate how different regulatory treatment is accorded for the modern sector. In 2011, China announced an investment of US$154 million to develop a cloud center for high-tech and start-up firms in Chongqing. The cloud computing Special Administrative Region (SAR) would be free from censorship.

The fundamental and proximate causes of prosperity/poverty and their relevance to cybercrime and cyber-security with special reference to China are presented in Table 2.

Table 2

Causes of prosperity and poverty and their relations to cyber-security orientation: examples from China

	Explanation	**Relevance to cyber-security in developing economies**	**Examples from China**
Fundamental causes of prosperity and poverty			
Political and economic institutions	• Institutions such as corruption, lack of accountability and weak law enforcement create bottlenecks for development [*63*] • National governments poorly equipped to deal with crimes • Weak democratic institutions	• Many governments, lack technological sophistication and are poorly equipped to fight the non-state criminal actors • Authoritarian regimes tend to focus more on cyber-control than on cyber-security	• China's cyberspace was less regulated: RBN's shift of operations to China • Congestion in law enforcement systems • Regulations geared towards cyber-control measures
Culture or informal institutions	• Sets of beliefs generated by some cultures may have anti-developmental consequences [*65*]	• Cybercrime are associated with a lower degree of stigmatization than in industrialized countries • Weak civil society	• Terms such as "hacker" and "hacking" have more positive and less negative connotations than in the West • Strong nationalism associated with cyber-wars • Roles of trade

	Explanation	Relevance to cyber-security in developing economies	Examples from China
			associations such as ISC have been limited in enhancing cyber-security
Proximate causes of prosperity and poverty			
Human capital	• Most developing economies fail to invest enough in education and skills	• Lack of cyber-security orientation of consumers and businesses	• Criminals have victimized naïve users and small businesses
Technology	• Developing economies tend to have low investment in R&D and low rate of adoption of technology • They also have a tendency to use low-cost technologies	• Low rate of adoption of cyber-security-related technology • Underdeveloped cyber-security industry • Low-cost technologies are more prone to cyber-threats	• A high proportion of users go online with crime prone technologies such as IE6

Political and economic institutions

China's political and economic system has important ramifications regarding the types of cyber-attacks that are controlled. One observation was that until not long ago, some aspects of China's cyberspace were less regulated than that of Russia. For instance, the notorious cybercrime organization, Russian Business Network (RBN) stopped operations in November 2007. Analysts suggested that the group operating RBN shifted its operations to China and other Asian countries [81]. China, however, subsequently tightened and restricted crime-enabling or facilitating institutions such as domain name registration.

China took the first major step toward criminalizing cybercrimes in February 2009 by including computer crimes in its Criminal Law. The punishment for hacking includes up to seven year prison sentence [82]. Gu Jian of the Chinese Ministry of Public Security noted that Chinese police shut down over 80 cybercriminal gangs during February 2009–October 2010 [20].

Since 2009 the Chinese government also tightened the registration requirements and processes for getting .cn domain names. The new rules do not allow individuals to register .cn domains. To register for businesses, it is required to submit a copy of the business license. Financially motivated Chinese cybercriminals, especially phishers, have been forced to register domains and subdomains that are easier and cheaper to obtain. The number of phishing attacks from .cn domains targeting Chinese businesses reduced from 2,826 in the second half of 2009 to 162 in the second half of 2010 [83]. Tighter regulations in China forced Chinese fraudsters to find poorly regulated top-level domains such as Tokelau domain (.tk) for phishing and spamming activities. In the third quarter of 2011, .tk domain registration was in the top 10 whereas .cn dropped off the top 10 list after declining for some time [84]. Among the 18,508 phishing attacks against Taobao.com in 2H 2011, 7,025 attacks had used maliciously registered domains names. Most were in .tk and only one .cn domain was registered for the purpose [28]

A society's power structure and the vested interests of powerful societal actors affect the way a cybercrime is defined and policed. China's state strategies with regard to ICTs have been to balance economic modernization and political control [85]. Stated simply, this strategy broadly corresponds to China's unique approach and perspective to cyber-security is reflected in the various cyber-control measures. Although about 40 governments control their online environments, few have done so more skillfully than by China [86]. The Chinese government has emphasized on healthy and harmonious Internet environment. A healthy cyberspace is "porn-free" and "crime-free" and "harmonious" means that it does not threaten to destabilize the state's social and political order.

It is also worth noting that the base of regime legitimacy in China has shifted from MarxLeninism to economic growth and prosperity [87]. China thus would like to achieve the goal of its cyberspace governance initiatives without jeopardizing its economic development [14].

Despite the tremendous difficulties associated with regulating and controlling the Internet, the Chinese government's cyber-control measures have been successful in some senses [88]. For instance, as presented in Fig. 5, China's share of global spam has decreased during 2007–2011. Spam messages originated from China in 2009 were 25 % less than in 2008 [89]. The reduction can be attributed to the country's regulations and enforcement mechanisms to tackle the spam problem. The government reportedly pressured Internet service providers to cut off their spam-sending accounts [89].

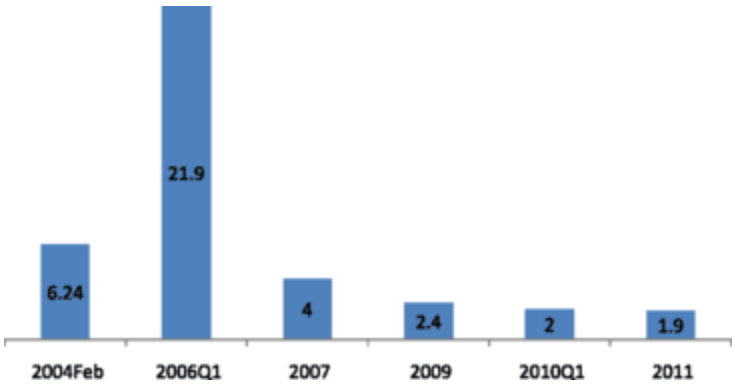

Fig. 5

China’s share of global spam (% of the world total). Sources: 2004: [90]; 2006: Sophos data from [91]; 2007:[74, 75]; 2009: [92]; 2010: [93]; 2011: [26]

That said the Chinese government has encountered a host of problems and difficulties associated with congestion in law enforcement and conflicts with economic modernization initiatives to achieve cyber-control related goals. First, consider the Green Dam Youth Escort firewall software program launched in 2008. The Chinese government had announced a plan to make it mandatory to have the Green Dam installed in all new PCs in the country. The stated goal of the mandate was to protect children from violent and pornographic contents.

The first problem the Green Dam faced was that while addressing one cyber-security issue, it created side effects that raised another. For instance, while it successfully blocked politically sensitive contents, many viewed that the software would represent significant risks to users as a single flaw the Green Dam system would expose the entire Chinese population to cybercriminals.

A second problem stemmed from the fact that it increased PC manufacturers’ costs, which led to an additional financial burden on consumers. While the Green Dam would be free to users, manufacturers needed to pay license fees to the Ministry of Industry and Information Technology (MIIT) to install the software. The vendor of the Green Dam, Beijing Dazheng Language and Knowledge Processing Research Center (BDLKPRC) had received $6 million from the MIIT to develop the software.

A third related problem had to do with strong opposition from computer manufacturers and the public. Even Lenovo, which is 57 % government-owned, opposed it. Internet users, who are increasingly acting on a bottom-up approach, participated in collective resistance efforts to abort the Green Dam.

Given the national security and economic risks and a strong resistance, the Green Dam program was indefinitely delayed after being installed in 20 million PCs. The unsustainable business model led to the closure of BDLKPRC in the 2010 and the company was near bankruptcy.

As another example, consider the 2011 regulation which required microbloggers to register using real name. The Nasdaq-listed Chinese online media company, Sina, warned that the requirement would negatively affect user activity and threaten its popular microblogging service, Sina Weibo. Even well after the March 16, 2012 deadline, Sina Weibo continued to allow users, who had not registered their real names to post and use its services.

As is the case of a number of other developing countries, China has weak democratic institutions [8], which have led to the various cyber-control measures discussed above. At the same time, despite China's fairly sophisticated cyber-control capabilities, the country's law enforcement resources have been insufficient to keep pace with the rapidly growing base of Internet users. In this way, as predicted by researchers in others fields [63], the weak law enforcement has created bottlenecks for the development of cyber-security.

Culture or informal institutions

Just like some sets of beliefs tend to have anti-developmental consequences [65], some aspects of culture help stimulate cybercrime behaviors in China.

A hacking culture

Recent studies and surveys have highlighted differences in culture associated with hacking in China and the West. For instance, many types of "hackers" are considered to be socially undesirable in the West [94]. The terms such as "hacker" and "hacking", on the other hand, seem to have somewhat more positive and less negative attitudes than they have acquired in the West. A significant proportion of Chinese students identify hackers as positive role models and some wish to emulate them. For instance, according to a 2005 Shanghai Academy of Social Sciences survey about 43 % of elementary school students said they "adore" China's hackers and about one third said they would like to be one [95]. Books and magazines on hacking appear to be more widespread and prevalent in China compared to elsewhere. For instance, magazines such as Hacker X Files and Hacker Defense provide step-by-step procedures and instructions for breaking into computers or writing malware. A "Hacker's Penetration Manual" reportedly cost less than US$6 [82]. There are also hacker clubs, hacker online serials, hacker conferences and hacker training academic institutions [95].

Strong nationalism

Probably one of the most interesting and intriguing features of cyber-attacks associated with China concern their links with the bases of nationalism. China's strong nationalism is arguably related to ethnicity and race rather than universalistic ideals (e.g., democracy, rule of law, free marketplace) and institutions [96]. In China, the state arguably has adapted a body of complex scholarship to bolster its legitimacy through invoking a deep sense of "Chineseness" among citizens [97–99]. In a review of literature, Sautman [100] 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". Observers note that Chinese hackers' nationalistic orientation and closeness to the state is an important way of distinguishing hacking activities originated from China. Chinese hackers consider their responsibility to protect their country and fight what they consider as imperialism in the cyberspace. Chinese hackers have expressed patriotic and nationalistic longings in several cyber-wars. Chinese hackers have fought cyber-wars with Taiwanese, Indonesians, Japanese and US hackers [51, 66, 101]. Thus when Chinese hackers see that the honor of their motherland is compromised, they consider it important to take necessary actions to restore their motherland's honor, glory and integrity.

A weak civil society

Although analysis of the state's contribution in promoting and/or inhibiting cyber-security as discussed above is worthwhile, it is important to understand the roles of the private sector and civil society. India would provide a particularly appropriate country for comparison. The active and influential roles played by India's National Association of Software and Service Companies (NASSCOM) have strengthened cyber-security orientation [6, 86]. Various ongoing efforts and activities initiated by the Data Security Council of India (DSCI) have helped enhance the country's cyber-security. One result of China's weak civil society and strong state is that trade and professional associations are likely to engaging in activities to promote the state's interest. The Internet Society of China (ISC) may be considered as the counterpart of the NASSCOM. For instance, in 2001 the ISC asked Internet companies to sign a voluntary pledge which required the signatories not to disseminate information "that might threaten state security or social stability" [102]. In 2009, China's dominant search engine, Baidu, and 19 other Internet companies received the "China Internet Self-Discipline Award". ISC Officials praised them for their roles in fostering, and supporting "harmonious and healthy Internet development" [103].

Human capital

The human development issue which is among the proximate causes of development [58] has special relevance for China's cyber-security. According to the McAfee cyber-defense survey of leading experts' perception of a nation's defenses released in January 2012, China is among the countries least able to defend against cyber-attacks. As discussed above cybercriminals have victimized naïve users and small businesses. As to the cognitive (e.g., knowledge about relevant cybercrime and cyber-security issues, how such knowledge is structured, and the way such knowledge is used to process information) and behavioral (the existence of healthy defensive and precautionary measures against cybercrime) orientations, as one might expect most Internet users in China are inexperienced and not technically savvy. Many Internet uses are unable to use IT security products developed in English language. Moreover, even if software companies publish security products in Chinese, they are unlikely to do so in all the dialects.

Technology

Some argue that networks in economies such as China have built-in security mechanisms as they have “wired security into their IT network infrastructure” compared to the Western approach of “bolting it on afterward to legacy systems” [104]. Contrary to this observation, China’s cyber-victimization, as is the case of most developing economies can be partly attributed to the country’s crime-prone technologies, the lack of absorptive capacity, a low level of national capabilities in the assimilation of technologies and associated organizational practices [67–69].

As noted above, developing economies such as China have a tendency to use low cost, but insecure technologies. According to Microsoft’s IE6Countdown website (http://www.ie6countdown.com/), as of November 2012, 6th version of Microsoft’s Internet Explorer (IE6) accounted for 21.3 % of browsers in China, which is the highest proportion in the world (Fig. 6). IE6 is reported to be inherently insecure and hacker-friendly browser. In 2006, for instance, Internet Explorer was reported to be unsafe for 284 days [105]. As indicated by prior researchers, China’s less developed information-security infrastructures make it attractive for hackers [27].

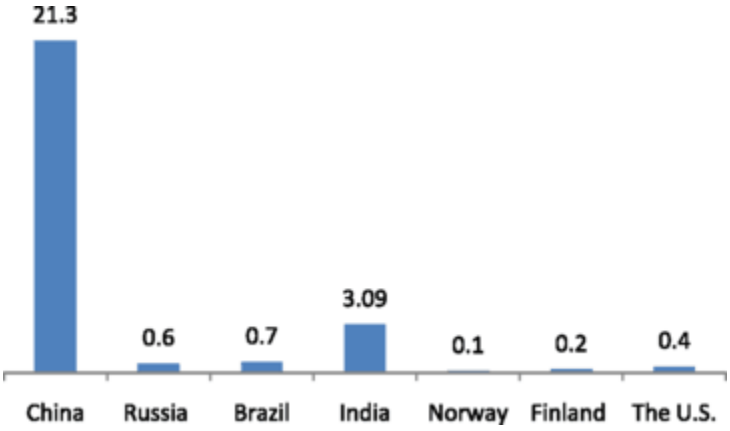

Fig. 6

A comparison of China’s Internet Explorer 6 usage with selected economies (November 2012). Source: The Internet Explorer 6 Countdown: moving the world off Internet Explorer 6, http://www.ie6countdown.com/

Developing country-based manufacturers also have a greater tendency to use cybercrime-prone pirated products to reduce the cost of PCs and other devices. The documents of a cyber-fraud lawsuit filed by Microsoft against a Chinese-owned domain provide a further glimpse into this phenomenon. Microsoft’s digital crimes unit investigating counterfeit software and malware had bought 20 new computers in China. The unit found counterfeit versions of Windows installed on all the machines and malware pre-installed on four of them. It was reported that in one of the brand new and direct from the factory condition laptops bought in Shenzhen, when it was booted up for the first time the Nitol virus was hidden in the laptop’s hard drive. The virus started

searching for another computer on the Internet. The laptop was made by a Guangzhou, China-based computer manufacturer, Hedy.

4.2 International relations/trade dimension of cybercrime and cyber-security associated with China

As observed by prior research (e.g., [*9*–*15*]), cyber-security is becoming an increasingly hot-button issue in China's political and economic relations with other economies. For one thing, China is facing unprecedented political and trade pressures from Western governments to combat and control cybercrimes allegedly originated from the country.

China and the Western countries, however, have differing viewpoints, assumptions and perspectives and hence differing objectives about cybercrimes associated with China. China has warned against what it refers as a "blame-game". In a letter to the editor of the Financial Times, Dai Qingli, Spokesperson, Chinese Embassy in the UK noted: "The only solution is through enhanced co-operation based on equality, mutual respect and mutual benefit, rather than politicising the issue or pointing fingers at others" [*106*].

Chinese officials argue that they should be praised, not criticized, for taking measures to control cybercrimes at home and collaborate at the international level. In contrast to the 1980s, China's central government leaders do not ignore or promote piracy and some other forms of cybercrimes [*107*]. In the early 2011, Chinese authorities and the US FBI conducted joint operations to dismantle and shut down an illegal website dealing with child pornography [*73*]. Qingli's letter to the editor of the Financial Times noted that Chinese police helped 41 countries investigate 721 cases related to cybercrimes between 2004 and 2010. She also said that China had inter-police co-operation with more than 30 countries [*106*].

China is also responding to the Western allegations by striking back with a strong denial and counter-allegation that US government agencies lack interest in fighting cybercrimes and do not cooperate with their Chinese counterparts. Gu Jian of the Chinese Ministry of Public Security noted that China had received no response in its request for cooperation from the US on 13 cybercrime cases involving issues such as fake bank websites and child pornography [*20*]. He further noted that in other cases it took up to six months to receive replies from the US.

<u>Alliance based on preferences related to cyberspace governance</u>

We can also observe new patterns of alliance based on cyber-security. Despite a broad agreement with the West on cybercrime, China diverges in several important respects of cyberspace governance. For one thing, China and some of its allies (Russia, Tajikistan and Uzbekistan) have different viewpoint of cyberspace governance. One such difference is their preference to tackle the broader problem of information security rather than cyber-security. In 2008, the Shanghai Cooperation Organization (SCO) Agreement in the field of International Information Security emphasized on and expressed concerns about the 'digital gap' between the West and the East.

These economies have been particularly concerned about the West's monopolization in ICT. The SCO economies like to control information that is likely to provoke what they call the three "evils" (terrorism, extremism, separatism). They also consider important to prevent other nations from using their technologies to disrupt economic, social and political stability. In September 2011, SCO economies submitted a draft International Code of Conduct for Information Security before the 66th UN General Assembly. Western countries, on the other hand, maintain that too much regulation may harm cyberspace security and emphasize the private sector's engagement [*108*].

While prior research suggests that countries' military alliance is positively related to trade relations due to possible security externalities and countries' motivations for helping their allies and punishing their enemies [*16, 72*], recent observations have indicated that alliances based on preferences related to cyberspace governance have strong implications for trades and investment in high technology products. An article published in China Economic Times on June 12, 2000 discussed three mechanisms that Xu Guanhua, then Chinese vice minister of the science and technology, thought high technology affects national security—military security, economic security, and cultural security. Regarding military security, Guanhua forcefully argued that developed countries have put many hi-tech arms into actual battles and discussed the likelihood of ICT exporting countries installing software for "coercing, attacking or sabotage".

More specifically, the Chinese government suspects that it is under cyber-attack from the US There has been a deep-rooted perception among Chinese policy makers that Microsoft and the US government spy on Chinese computer users through secret "back doors" in Microsoft products. Computer hardware and software imported from the US and its allies are subject to detailed inspection. Chinese technicians take control of such goods and either resist or closely monitor if Western experts install them [*109*]. Chinese cryptographers reportedly found an "NSA Key" in Microsoft products, which was interpreted as the National Security Agency. The key allegedly provided the US government back-door access to Microsoft Windows 95, 98, N-T4, and 2000. Although Microsoft denied such allegation and even issued a patch to fix the problem, the Chinese government has not been convinced.

Chinese high technology companies are facing similar barriers to trade and investment in Western countries. In the Chinese PC maker Lenovo's acquisition of IBM's PC division, the former's connection to the Chinese government was one of the biggest roadblocks facing the company. National security was a matter of top concern for the US government. Some US lawmakers argued that the deal could lead to a transfer of IBM's advanced technology and other corporate assets to the Chinese government. The issue surfaced again in 2006, when critics challenged Lenovo's sale of 16,000 desktop computers to the US State Department. Politicians and some commentators drew attention to the potential negative national security implications of placing Chinese computers into government offices. They argued that the company's connections to the Chinese government could pose a security risk. Another Chinese high technology company, Huawei faced similar barriers in Australia, India, and the US.

5 Discussion and implications

We developed typology and looked at the developmental and international aspects of cybercrime and cyber-security issues associated with China. The typology would help understand cybercrime logic so that various actors interested in fighting cybercrimes can adapt the responses to the nature of cybercrimes and criminals involved. For instance, the differences in cybercrimes have important consequence for the government's cybercrime fighting measures. Such an approach would also be useful for understanding circumstances, for a simple non-organized cyber-offence such as simple hacking as well as more organized cyber-attacks.

The degree of sophistication and complexity of cyber-attacks that are believed to originate from China is intriguing. Cyber-attacks originating from China arguably have caused substantial economic damage to the Western economies. Viewed against the backdrop of China's growing size, influence and power, however, Western actors have limited leverage over China-originated cybercrimes. For instance, given the current state of China-US relationship, it will be next to impossible for a Chinese cybercriminal to get extradited to the US.

While nationalism issues have been identified in some domestic cyber-attacks, nationalism-driven legitimacy to cyber-attacks is especially prevalent in those that target foreign websites. Professional organizations such as the Honker Union of China (or the Red Hackers) also provide legitimacy to such attacks. Many patriotic hackers learned important skills and felt more capable of attacking networks for financial motivations. The Chinese economy is also becoming attractive for extrinsically motivated cybercriminals. Our findings are contrary to the widely accepted belief that Chinese hackers mainly focus on foreign consumers. In view of the increasing problems caused by extrinsically motivated cybercrimes, more cyber-police initiatives may have to be redirected to fight such crimes.

Alleged cyber-attacks from China have been among the major forces that is increasingly shaping institutions in the US and other industrialized countries. Measures are being taken to make cyber-attacks an integral part of risk assessment. In the 10-k reports filed with the US Securities and Exchange Commission (SEC), DuPont did not identify hacking a risk and provided no indication that the company was an industrial espionage victim. As noted above, Google announced that China-originated attacks that infiltrated the company attacked at least 34 other major companies. While two, Intel and Adobe confessed, albeit with few specifics, no other companies stepped forward [*40*]. Given the perception of high-profile cyber-attacks originating from China, investors may no longer tolerate organizations' hesitant and secretive mentalities and unwillingness to report cyber-attack victimization.

On the bright side, Chinese firms have increased investments in IT security products, which can be considered as a positive and encouraging sign. IDC estimated that China's IT security market crossed US$300 million in 2010 [*110*]. Estimates of CCID Consulting suggested that China's

information security product market would experience a compound annual growth rate of 21.5 % during 2010–2012.

There have also been a plethora of collaborations, co-operations and partnerships between local companies, which have helped enhance cyber-security measures [*86*]. For instance, the gaming company, Tencent shares a cloud-computing security platform with Kingsoft [*111*].

Government-industry collaborations have also culminated in China's new cyber-security initiatives. The Chinese government is working with search engines such as Baidu and Sohu and financial institutions to prevent phishing attacks. The top Chinese search engines are persuaded to take new anti-phishing measures. Some search engines promised that their search results would display a special icon next to the legitimate websites of banks and other financial institutions to differentiate them from bogus websites [*49*]. Moreover, when users search for related keywords, the official websites of financial institutions such as Agricultural Bank of China and China Construction Bank would be ranked first.

6 Concluding comments

A complex interaction of international and domestic politics and economics has shaped cybercrimes originating from and affecting China as well as the patterns of cyber-security measures. Informal institutions in China are more supportive and less hostile to cybercrimes compared to those in the West and some other developing countries. China undoubtedly has comprehensive cyber-security initiatives. A great deal of attention is, however, devoted to deal with issues that the Chinese government considers important and urgent. For instance, the emphasis on creating and promoting healthy and harmonious Internet environment has led to the development of sophisticated monitoring and control systems.

References

Goldsmith, E., & McGregor, S. L. T. (2000). E-commerce: consumer protection issues and implications for research and education. *Journal of Consumer Studies & Home Economics, 24*(2), 124–127.

Narayanasamy, K., Rasiah, D., & Tan, T. M. (2011). The adoption and concerns of e-finance in Malaysia. *Electronic Commerce Research*, *11*(4), 383–400.

Antoniou, G., & Batten, L. (2011). E-commerce: protecting purchaser privacy to enforce trust. *Electronic Commerce Research*, *11*, 421–456.

Lu, J., Wang, L. Z., Yu, C. S., & Wu, J. Y. (2009). E-auction web assessment model in China. *Electronic Commerce Research*, *9*(3), 149–172.

Taylor, D. G., Donna, F. D., & Jillapalli, R. (2009). Privacy concern and online personalization: the moderating effects of information control and compensation. *Electronic Commerce Research*, *9*(3), 203–223.

Kshetri, N. (2010). Cloud computing in developing economies. *Computer*, *43*(10), 47–55.

Kshetri, N. (2010). *The global cyber-crime industry: economic, institutional and strategic perspectives*. Berlin: Springer.

UNDP (2006). Country evaluation: assessment of development results Honduras. New York: United Nations Development Programme Evaluation Office. http://web.undp.org/evaluation/documents/ADR/ADR_Reports/ADR_Honduras.pdf.

Andreas, P., & Price, R. (2001). From war fighting to crime fighting: transforming the American national security state. *International Studies Review*, *3*(3), 31–52.

Collins, A. (2003). *Security and southeast Asia: domestic, regional and global issue*. Boulder: Lynne Rienner Pub.

Frost, E. L., Przystup, J. J., & Saunders, C. P. (2008). China's rising influence in Asia: Implications for US Policy. Institute for National Strategic Studies (INSS), Washington DC, United States. http://www.isn.ethz.ch/isn/Digital-Library/IR-Directory/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=13298.

Griffith, I. L. (1993). Drugs and security in the commonwealth Caribbean. *Journal of Commonwealth & Comparative Politics*, *31*(2), 70–102.

Wenping, H. (2007). The balancing act of China's Africa policy. *China Security*, *3*(3), 32–40.

Kshetri, N. (2013, forthcoming). Cyber-victimization and cybersecurity in China. *Communications of the ACM*.

Kshetri, N. (2013, forthcoming). *Cybercrime and cybersecurity in the Global South*. Basingstoke, UK: Palgrave Macmillan.

Gowa, J. (1994). *Allies, adversaries, and international trade*. Princeton: Princeton University Press.

Schafer, S. (2006). A piracy culture; Beijing continues to defy US and European efforts to stop IP theft. *Newsweek International*.

Xinxin, Z. (2012). China to Further Safeguard Cyber Security. 13 January. http://english.peopledaily.com.cn/90882/7704949.html. Accessed 12 May 2012.

chinadaily.com (2012). Internet population grows amid concerns. 11 January. http://www.chinadaily.com.cn/china/2012-01/11/content_14424818.htm.

China Daily (2010). 2010 Internet policing hinges on transnational cybercrime. 10 November. http://www.china.org.cn/business/2010-11/10/content_21310523.htm.

Riptech (2002). Riptech Internet Security Threat Report (Vol. II). July. http://www.4law.co.il/276.pdf. Accessed 27 Oct 2005.

Lindenmayer, I. (2006). Online. *American Banker, 171*(18), 6.

Greenberg, A. (2007). The top countries for cybercrime. Forbes.com. 17 July. http://www.forbes.com/2007/07/13/cybercrime-world-regions-tech-cx_ag_0716cybercrime.html. Accessed 9 Apr 2008.

Pauli, D. (2012). China named 'world's biggest' cybercrime victim. 23 March. http://www.crn.com.au/News/294695,china-named-worlds-biggest-cybercrime-victim.aspx.

Microsoft.com (2012). Microsoft security intelligence report, Volume 13. January through June. www.microsoft.com/sir.

sophos.com (2012). Security threat report. http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.ashx.

Microsoft (2011). Microsoft security intelligence report. http://www.microsoft.com/security/sir/keyfindings/default.aspx#!section_4_1_d.

Aaron, G., & Rasmussen, R. (2012). Global phishing survey: trends and domain name use in 2H2011. In *APWG*, April 26.http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf.

Kim, S. H., Wang, Q., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM*, *55*(3), 66–73.

Fletcher, O. (2009). China game boss sniped rivals, took down Internet. 28 August.http://www.pcworld.com/businesscenter/article/171018/china_game_boss_sniped_rivals_took_down_internet.html. Accessed 12 May 2012.

Fletcher, O. (2009). China jails Trojan virus authors in cybercrime crackdown: arrests and jail time for cybercriminals are increasingly common in China. 16 December. http://www.networkworld.com/news/2009/121709-china-jails-trojan-virus-authors.html. Accessed 12 May 2012.

Schwartz, M. J. (2011). 111 arrested in identity theft probe. *InformationWeek*.http://www.informationweek.com/news/security/attacks/231900438. Accessed 12 May 2012.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, *44*, 588–608.

Hindelang, M., Gottfredson, M., & Garofalo, J. (1978). *Victims of personal crime: an empirical foundation for a theory of personal victimization*. Cambridge: Ballinger.

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

bbc.co.uk (2011). Chemicals and defense firms targeted by hacking attack. 31 October. http://www.bbc.co.uk/news/technology-15529930.

Pelofsky, J. (2011). Chinese man gets prison for US trade secrets theft. http://www.chicagotribune.com/news/sns-rt-us-crime-china-thefttre7bk2a4-20111221,0,6950261.story. Accessed 12 May 2012.

Noga, E. (2010). I spy something rubber. *Rubber & Plastics News*, *40*(7), 1.

ncix.gov (2011). Foreign spies stealing US economic secrets in cyberspace. Office of the National Counterintelligence Executive, Washington, DC. October. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf Accessed 8 Nov. 2011.

Riley, M. (2012). SEC push may yield new disclosures of company cyber attacks. 10 January. http://www.businessweek.com/news/2012-01-10/sec-push-may-yield-new-disclosures-of-company-cyber-attacks.html

Chirgwin, R. (2011). Feds finger China in wire fraud: Where phishing victims' money goes. 26 April.http://www.theregister.co.uk/2011/04/26/feds_finger_china/.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*, 13–20.

Hamid, T. (2011). Smart devices prey for cybercrime. *MEED. Middle East Economic Digest*, *55*(2), 25–26.

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

Information Warfare Monitor/Shadow server Foundation (2010). *Shadows in the cloud: investigating cyber espionage 2.0*. Joint report: Information Warfare Monitor Shadowserver Foundation, JR03-2010, 6 Apr. www.utoronto.ca/mcis/pdf/shadows-in-the-cloud-web.pdf.

McMillan, R. (2010). More than 100 companies targeted by Google hackers. 27 February.http://www.computerworld.com/s/article/9163158/More_than_100_companies_targeted_by_Google_hackers.

McDonald, J. (2011). Cyber attacks on chemical companies traced to China.http://www.usatoday.com/money/industries/technology/story/2011-11-01/China-hackers/51024936/1. Accessed 12 May 2012.

Blitz, J. (2011). Security: a huge challenge from China, Russia and organised crime. 1 November. http://www.ft.com/intl/cms/s/0/b43488b0-fe2a-11e0-a1eb-00144feabdc0.html#axzz1dnezI1eF.

bbc.co.uk (2011). China seeks to combat hi-tech crime wave. 30 December. http://www.bbc.co.uk/news/technology-16357238.

Roberts, D. (2008). Inside the war against China's blogs; vengeful bloggers? Flaming posts? PR firms help global brands navigate the country's perilous web. *Business Week*, *4089*, 60.

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.

washingtonpost.com (2012). Global police network Interpol to make war on cyber criminals a priority. May 8.http://www.washingtonpost.com/business/global-police-network-interpol-to-make-war-on-cyber-criminals-a-priority/2012/05/08/gIQARD4RAU_story.html. Accessed 12 May 2012.

Guillén, M. F., & Suárez, S. L. (2005). Explaining the global digital divide: economic, political and sociological drivers of cross-national Internet use. *Social Forces*, *84*(2), 681–708.

Lewis, A. (1954). Economic development with unlimited supplies of labour. *Manchester School of Economic and Social Studies*, *XXII*, 139–191.

Hasan, I., & Kobeissi, N. (2012). Innovations, intellectual protection rights and information technology: an empirical investigation in the MENA region. *Electronic Commerce Research*, *12*, 455–484.

Cetron, M. J., & Davies, O. (2009). Critical trends for cyber security. *The Futurist*, *43*(5), 40–49.

Chenery, H. B. (1975). The structuralist approach to development policy. *The American Economic Review*, *65*(2), 310–316. Papers and proceedings of the eighty-seventh annual meeting of the American Economic Association.

Acemoglu, D. (2005). Political economy of development and underdevelopment. Gaston Eyskens lectures, Leuven, Department of Economics, Massachusetts Institute of Technology. http://economics.mit.edu/files/1064.

Acemoglu, D., Johnson, S., & Robinson, A. J. (2005). Institutions as a fundamental cause of long-run growth. In P. Aghion & S. N. Durlauf (Eds.), *Handbook of economic growth*, *IA*,

Amsterdam: Elsevier. http://baselinescenario.files.wordpress.com/2010/01/institutions-as-a-fundamental-cause.pdf.

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

Jones, E. L. (1981). *The European miracle: environments, economies, and geopolitics in the history of Europe and Asia*. New York: Cambridge University Press.

Roland, G. (2004). Understanding institutional change: fast-moving and slow-moving institutions. *Studies in Comparative International Development, 28*(4), 109–131.

De Laiglesia, J. R. (2006). *Institutional bottlenecks for agricultural development a stock-taking exercise based on evidence from Sub-Saharan Africa* (Working Paper No. 248). OECD Development Centre, Research programme on: policy analyses on the institutional requirements for advancing peace and development in Sub-Saharan Africa. http://www.oecd.org/dev/36309029.pdf.

Andreas, P. (2011). Illicit globalization: myths, misconceptions, and historical lessons. *Political Science Quarterly*, *126*(3), 403–425.

Greif, A. (1994). Cultural beliefs and the organization of society: a historical and theoretical reflection on collectivist and individualist societies.*Journal of Political Economy*, *102*, 912–950.

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

Cohen, W., & Levinthal, D. (1990). Absorptive capacity: a new perspective on learning and innovation. *Administrative Science Quarterly, 35*, 128–152.

Dahlman, L., & Nelson, R. (1995). Social absorption capability, national innovation systems and economic development. In B. H. Koo & D. H. Perkins (Eds.), *Social capability and long-term growth* (pp. 82–122). Basingstoke, UK: Palgrave Macmillan.

Niosi, J. (2008). Technology, development and innovation systems: an introduction. *The Journal of Development Studies*, *44*(5), 613–621.

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

Pearlstine, N. (2012). Life in Cyberia. *Bloomberg Businessweek, 4291*, 48–54.

Milner, H. V. (1999). The political economy of international trade. *Annual Review of Political Science, 2*, 91–114.

Lan, T. (2011). Real rules for virtual space. *Beijing Review, 54*(47), 12–13.

Kshetri, N. (2009). The evolution of the Chinese online gaming industry. *Journal of Technology Management in China*, *4*(2), 158–179.

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

Fong, C. (2008). Fighting the agents of organized cybercrime. 8 May. CNN.com.

China Daily (2008). China gets its game on 5 May. http://www.chinadaily.com.cn/bizchina/2008-05/05/content_6661519.htm. Accessed 2 Oct. 2008.

chinadaily.com.cn (2012). China's online gaming market reports 32 % revenue increase. 10 January. http://www.chinadaily.com.cn/china/2012-01/10/content_14415239.htm. Accessed 12 May 2012.

Nystedt, D. (2004). Online gaming growing fast in China, study says.http://archive.thestandard.com/movabletype/datadigest/archives/003210.php. Accessed 27 Oct 2005.

Mims, C. (2012). Chinese cyber-criminals caught laundering $48 m through online games. 17 October. http://qz.com/16717/chinese-cyber-criminals-caught-laundering-48-mln-through-online-games/.

Blakely, R., Richards, J., & Halpin, T. (2007). Cyber gang raises fear of new crime wave. *The Times*, 13. November 10.

Barboza, D. (2010). Hacking for fun and profit in China's underworld. 1 February.http://www.nytimes.com/2010/02/02/business/global/02hacker.html?pagewanted=all.

Rashid, F. Y. (2011). Cyber-criminals register free domains and subdomains for phishing attacks. 27 April.http://www.eweek.com/c/a/Security/CyberCriminals-Register-Free-Domains-and-SubDomains-for-Phishing-Attacks-470147/. Accessed 12 May 2012.

Rashid, F. Y. (2011). Internet expands to 220 million domains: VeriSign. 23 December. http://www.eweek.com/c/a/Security/Internet-Expands-to-220-Million-Domains-VeriSign-406627/. Accessed 12 May 2012.

Kalathil, S. (2003). China's new media sector: keeping the state in. *The Pacific Review*, *16*(4), 489–501.

Kshetri, N. (2013, forthcoming). Privacy and security issues in cloud computing: the role of institutions and institutional evolution.*Telecommunications Policy*. doi:10.1016/j.telpol.2012.04.011

Zhao, S. (2000). Chinese nationalism and its international orientations. *Political Science Quarterly*, *115*(1), 1–33.

Wu, G. (2009). In the name of good governance: e-government, Internet pornography and political censorship in China. In X. Zhang & Y. Zheng (Eds.), *China's information and communications technology revolution: social changes and state responses* (pp. 69–83).

Greenberg, A. (2009). Brazil: the new spam king. Forbes.com. 8th December. http://www.forbes.com/2009/12/08/spam-china-cisco-technology-cio-network-brazil.html.

Sophos (2004). Sophos outs 'dirty dozen' spam producing countries. 26 February. http://www.sophos.com/en-us/press-office/press-releases/2004/02/sa_dirtydozen.aspx. Accessed July 2011.

Theregister.co.uk (2006). China poised to pinch US spam crown. 21 April. http://www.theregister.co.uk/2006/04/21/spam_relay_hotlist/.

Trupela Tok (2010). Spam statistics for 2009. 5 January. http://www.trupela.com/2010/01/05/spam-statistics-for-2009/.

Secure List (2010). Spam evolution: January-March 2010. 12 May.http://www.securelist.com/en/analysis/204792117/Spam_evolution_January_March_2010.

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

Hvistendahl, M. (2009). The China syndrome. *Popular Science*, *274*(5), 60–65.

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

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

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

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

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

Denning, D. E. (2000). Hacktivism: an emerging threat to diplomacy. American Foreign Service Association.www.afsa.org/fsj/sept00/Denning.cfm. Accessed 1 Oct 2009.

The Economist (2002). Asia: stop your searching; the Internet in China. 7 September, 68.

MacKinnon, R. (2012). Inside China's censorship machine. 29 January. http://fullcomment.nationalpost.com/2012/01/29/rebecca-mackinnon-inside-chinas-censorship-machine/.

Hawser, A. (2011). Hidden threat. *Global Finance*, *25*(2), 44.

Krebs, B. (2007). Internet Explorer unsafe for 284 days in 2006. 4 January.http://blog.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html.

Qingli, D. (2011). China itself is facing growing cybercrime and attacks. 11 November. http://www.ft.com/intl/cms/s/0/2a134f8c-f5be-11e0-bcc2-00144feab49a.html#axzz1dOy0Cfug. Accessed 12 May 2012.

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

Kizekova, A. (2012). The Shanghai Cooperation Organization: challenges in cyberspace—analysis. http://www.eurasiareview.com/27022012-the-shanghai-cooperation-organisation-challenges-in-cyberspace-analysis/. Accessed 12 May 2012.

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

IDC (2011). China IT security solutions: an IDC report series. http://www.idc.com/getdoc.jsp?containerId=IDC_P10684.

Tsuruoka, D. (2012). Tencent, Kingsoft to run online games together. March 13.http://news.investors.com/article/604133/201203131136/tencent-kingsoft-form-online-game-alliance.htm. Accessed 12 May 2012.