Cybersecurity and International Relations: The U.S. Engagement with China and Russia

Nir Kshetri, The University of North Carolina at Greensboro

Prepared for FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, Argentina, July 23-25

Please send correspondence to:

Nir Kshetri
The University of North Carolina at Greensboro
The Bryan School of Business and Economics
PO Box 26170, Greensboro, NC 27402-6170
E-mail: NBKSHETR@uncg.edu
Cybersecurity and International Relations: The U.S. Engagement with China and Russia

Abstract
Cybersecurity-related institutions at the international levels are evolving. In this article we draw on theories, concepts, practices and findings from organizational theory, game theory and international relations to examine the cybersecurity-related international engagements. This paper also investigates how the nature of the cyberspace is likely to act as a major source of international conflicts. We examine the challenges associated with formal treaties and frameworks as well as informal cooperation related to cybersecurity. Various sources of conflict and tension in cybersecurity-related international relations have been identified. Also analyzed in the paper are the conditions that have led to the lack of cooperation from China and Russia in the U.S. request to extradite Edward Snowden, the whistleblowing former CIA employee. Several key issues unresolved in the literature are highlighted.

Keywords: Cybersecurity; international relations; national security; formal treaties; informal cooperation; Russia; China

Introduction
The cyberspace has added new dimensions and complexity to national security and international relations. Almost a decade and a half ago, Cobb (1999) observed that the conflicts involving the cyberspace are the most serious national security threats facing nations since the development of nuclear weapons in the 1940s. Protecting the cyberspace has been a top concern for many governments. An Economist article noted: “After land, sea, air and space, warfare has entered the fifth domain: cyberspace” (economist.com, 2010).

A high profile example of a new international conflict created by issues involving cybersecurity could be recent developments involving Edward Snowden’s leaks of classified documents about the U.S. government’s surveillance programs. Russia and China refused to comply with U.S. requests to extradite Snowden. Hong Kong, a Special Administrative Region (SAR) of China, showed a clear lack of cooperation, contending that “the documents provided by the U.S. Government did not fully comply with the legal requirements under Hong Kong law”. Despite a fierce opposition by the Obama Administration, Russia granted him temporary
residence permit. While the Obama Administration has accused Snowden of espionage, leaders of both China and Russia praised his role and decision in revealing the details of the U.S. National Security Agency's (NSA) secret surveillance program. Providing support for the activities of Snowden and the WikiLeaks founder Julian Assange, Russian President, Vladimir Putin put the issue this way: "Assange and Snowden consider themselves human rights activists and say they are fighting for the spread of information. Ask yourself this: should you hand these people over so they will be put in prison?" (Elder and Kaiman, 2013). Likewise, a main heading in the front page of the overseas edition of the People's Daily, the official newspaper of the Chinese Communist Party (CCP), noted that Snowden’s "fearlessness … tore off Washington's sanctimonious mask". A commentary in the Global Times, owned by the People's Daily, also attacked the U.S. forcornering "a young idealist who has exposed the sinister scandals of the US government". In a related development, the Brazilian President Dilma Rousseff indefinitely postponed her state visit to the U.S., which was planned for October 2013. She expressed anger and frustration that the NSA had allegedly intercepted her private communications, hacked into the state-owned Petrobras oil company's network and spied on Brazilians who had their personal data stored in the networks of U.S. companies such as Facebook and Google (Brooks and Bajak, 2013). Quoting the White House, a New York Time article reported that “Obama expressed regret over the spying on an ally” (Shear, 2013).

In general, efforts of the U.S. to gain broad international support on cybersecurity related matters have met with very limited success. For instance, consider the World Conference on International Telecommunications (WCIT-12) convened by the International Telecommunication Union (ITU) in December 2012 to amend the International Telecommunication Regulations (ITRs) treaty, which was adopted in 1988. The U.S. opposed the treaty arguing that it would
increase the governmental oversight and control of the cyberspace. Of the 144 countries with the voting rights at the WCIT-12, eighty-nine countries or two thirds of ITU members signed the revised ITRs, which included many countries in Africa and the Middle East, Brazil, Mexico, Argentina, China, Indonesia, Iran, and Russia. Only fifty-five countries including Australia, India, members of the European Union (EU), Canada, Japan, and the U.S. did not sign the treaty (ITU, WCIT, 2012).

As cyber offense and defense capabilities continue to develop rapidly, various issues related to cyberspace policies and practices will become of increasing significance and will require comprehensive national security and international relations strategies. From the national security and international relations standpoint, there are a number of unique aspects of the cyberspace which may offer some insight into some of the major and new conflicts among nations as noted above. First, the limited success in cybersecurity related cooperation can be attributed to the lack of rules and norms of engagement in the cyberspace-related matters. For instance, while a host of unspoken understandings guided the U.S.-Soviet Union relations (Lipson, 1991), due to the newness of this phenomenon, similar types of understandings have not yet developed to guide international relations on the cyberspace due to its newness.

Second, most of the suggestions regarding nation states’ involvement in cyberattacks against other countries are generally inferred from circumstantial rather than direct, factual and conclusive evidence. A powerful example to illustrate this is the Stuxnet virus, which was programmed to damage Iran's centrifuges at the Natanz nuclear site (Rid, 2012). While Israel and the U.S. have been blamed as creators of the virus, the nature of the cyberspace makes it impossible to trace the actual origin of the software (Choucri and Goldsmith, 2012).
Third, nations may commit more frequent violations in the cyberspace compared to the physical space. This is because the nature of the cyberspace makes it easier to discredit the evidence presented by the adversaries. A related point is that violators are very rarely punished. Prior researchers have suggested that actors are likely to engage in violations if such violations cannot be witnessed and violators go unpunished (Lipson, 1991; Ramseyer, 1991).

So far we have no definite answer to the question of whether the Global Information Age is likely to pose a critical challenge to state power (Simmons, 2011). In order to understand how the information age has presented both an opportunity and a challenge to the state power, consider the sophisticated cyberespionage network tracked in 2010 by U.S.- and Canada-based researchers, which they referred as the Shadow network (Information Warfare Monitor/Shadowserver Foundation, 2010). The targets included the Indian Ministry of Defense, the U.N., and the Office of the Dalai Lama (Kshetri, 2010). For instance, malware installed in the computers of the Dalai Lama’s Office turned on the microphones and cameras, controlled keyboards, and downloaded emails (Simmons, 2011). Regarding the perpetrator behind the attacks, the fact that Wikileaks pointed to the Chinese government rather than the mainstream media is illustrative of how the abilities of so called “techno-libertarians” to expose the secrets of a major state (Kazan, 2010).

Our purpose in this paper is to illustrate this complexity. Specifically, we focus on the relationships of the U.S. with China and Russia in issues involving cybersecurity. This paper makes several contributions to the literature on international relations and national security. First, the Information Age has also offered governments a number of possible ways to weaken their opponents (Simmons, 2011). Many governments are weighing such possibilities. The Information Age, however, is clearly a double-edged sword. Nye (2011) predicted that the
diffusion of power in the Information Age is likely to be much more challenging for states than
the rival states’ rise. In light of this observation, the current paper seeks to enrich and expand
research in this area by synthesizing evidence, concepts and knowledge from a number of
disciplines to explore how nations are recognizing opportunities that have emerged from the
rapid developments of information and communications technologies (ICTs) and dealing with
challenges that are presented by such developments.

Second, scholars have emphasized the importance of improving our understanding of
various mechanisms of informal influence available to powerful states in international
organizations, which is vital to clarify predictions about states' choice of one mechanism over
another (Hawes, 2004). Understanding these various mechanisms, and when and how powerful
states use them, will go a long way towards providing one of the missing pieces in current
scholarship on state power and international organization (Hawes, 2004). In this regard, this
study provides new insights into the effectiveness and limitations of informal cooperation in
cybersecurity-related international relations.

Third, researchers have pointed out that there is a disconnection between research on
international relations and national policies regarding states’ engagement in the cyberspace
(Choucri and Goldsmith, 2012). Our findings would help policy makers understand the
complexity, dynamics, uncertainty and demands of the cyberspace.

The paper is structured as follows. We proceed by first comparing the effectiveness of
formal treaties and frameworks and informal cooperation in cybersecurity-related international
relations. Then, we examine the U.S. relationships with China and Russia in issues involving the
cyberspace. Next, we discuss the critical issues and areas of disagreement. It is followed by
sections on the potential and the way forward; and discussion and implications. The final section provides concluding comments.

**Formal treaties and frameworks versus informal cooperation in cybersecurity**

Treaties involving alliances and broad policy guidelines are sustained only by perceptions of mutual advantage (Baxter, 1980). The Council of Europe (CoE) treaty, which is the most well-known treaty on cybercrime, has not been able to attract the support of a large number of countries. In addition to the general Western focus, many countries have objected to a number of clauses of the Treaty including definitions of cybercrimes, criminalization of intellectual-property rights violations, mechanisms that involve intrusion of national sovereignty (Goldsmith, 2011; Keyser, 2003). In this regard, China, Russia and many developing countries have seen no advantage of the CoE Treaty.

From the U.S. perspective, it is also important to note that the focus of the country is shifting away from formal multilateral processes towards informal mechanisms. Especially, the Obama administration’s approach to international cooperation has been through ad hoc or informal mechanisms that have bypassed and ignored formal institutions and treaties (Skidmore, 2012). For instance, through June 2010, the Obama administration had submitted only six treaties to the Senate, only one of which was multilateral in scope. Except for the bilateral New START Treaty, which seeks to reduce U.S. American and Russian nuclear arsenals, the treaties were minor (Skidmore, 2012). While Russia favors an international treaty to secure cyberspace against threats, the U.S. is interested in promoting more intimate cooperation among international law-enforcement officials.

An important question, then, is whether informal institutions perform better than the formal ones in dealing with international problems related to the cyberspace. Before proceeding
further, let us note first some criticisms that have been made of informal networks. Critics have argued that participation in such networks is voluntary rather than compulsory, engagement varies considerably across nations, and the bodies that coordinate such networks lack formal enforcement powers and mission-critical services to compliance. Prior researchers have suggested that informal cooperation is unlikely have a significant effect on domestic policy (Downs, Rocke and Barsoon, 1996; Drezner, 2007).

Despite criticisms by some doubters such as those outlined above the diversity, scale and variation of informal networks and agreements among states and transnational actors indicate that they are an important feature of the world politics (Lipson, 1991). Prior researchers have suggested that trans-governmental networks consisting of domestic regulators and public officials—as a form of informal institution—are becoming an increasingly common feature of global governance (Bach and Newman, 2010). Such networks are found in a number of areas such as financial markets, aviation, antitrust, data privacy, pharmaceuticals, and the environment (Bach, 2010; Bermann, 1993; Cardenas, 2003; Newman, 2008; Thurner and Martin, 2009). State and sub-state officials from a number of countries work together to share information with each other, develop harmonized guidelines and best practices, and reduce friction associated with globalization (Bach and Newman, 2010). Slaughter (2000, 204) argues that these networks are “the optimal form of organization for the Information Age”. Such informal networks have become a common mechanism for solving foreign originated cybercrimes.

Lipson (1991, p. 500) suggested that "informal bargains are more flexible than treaties" since they are "willows, not oaks" and can be adapted to meet uncertain conditions and unpredictable shocks. The Snowden case and many similar events suggest that countries are increasingly subjected to unpredictable shocks in the digital age. Thus international informal
agreements may serve as a better choice than formal instruments in addressing many significant issues involving cyber-conflicts.

Prior researchers have recognized various forms of informal influence. They include withholding of or stopping financial contributions to international organizations, threats to disengage or actual dis-engagement from networks and alliances and engagement in covert activities to influence negotiations or affect bargaining advantage (Hawes, 2004). Informal networks have been shown to be effective in changing behaviors of institutional actors in foreign countries. For instance, Bach and Newman (2010) found that participation in the trans-governmental securities network is positively related to a jurisdiction’s adoption and enforcement of insider-trading rules. They found that a MoU type of collaboration or similar agreement with the U.S. Securities and Exchange Commission (SEC) makes a jurisdiction four times more likely to adopt insider-trading regulation. They also found that the relationship between network-based cooperation and domestic regulatory practice is more complex and different network components are associated with different outcomes (Bach and Newman, 2010).

Moving to the specific context of the cyberspace, informal networks have become a significant force in fighting international cybercrimes. The U.S. FBI announced in 2009 that it would permanently base a cybercrime expert in Estonia. As an example of significant success, working closely with the Estonian Police and Border Guard, the Dutch National Police and other organizations, the FBI solved a high profile click hijacking case, which involved a crime ring consisting of six Estonians and one Russian. The ring was estimated to generate at least US$14 million in profits. Estonia also extradited the six Estonians involved in the fraud to the U.S. (Kshetri, 2013).
As another example, the Romanian Directorate for Investigating Organized Crime and Terrorism (DIICOT) reported that it exchanged information with law enforcement agencies from more than 50 countries such as the U.K.’s Serious Organized Crime Agency (SOCA) and the FBI (Constantin, 2011). As a further example, since 2009, the FBI has stationed a special agent at the U.S. Embassy in Ukraine for assisting investigations of cybercrime targeting the U.S. (Kirk, 2012). The Ukrainian law enforcement agencies have cooperated with the U.S. on cybercrime investigation. In October 2010, Ukraine’s Security Service of Ukraine (Sluzhba Bezpeky Ukrayiny, or SBU) in cooperation with law enforcement agencies from the U.S., U.K. and the Netherlands arrested five alleged kingpins of a criminal group, which stole US$ 70 million from U.S. bank accounts (Onyshkiv and Bondarev, 2012).

Actors with relatively high bargaining power, who possess ability to make credible threats may change informal institutions in their favor (Farrell and Héritier, 2003). For instance, U.S. diplomats have admitted the use of foreign aid to influence key votes in the U.N. General Assembly (Hawes, 2004). An actor’s relative power, on the other hand, is a function of its place in formal institutions, the time horizons under consideration, sensitivity to failure and its level of resources (Farrell and Héritier, 2003). Whereas factors such as the economic strength and possession of nuclear weapons became important sources of a nation's bargaining power in international affairs, these factors have become less relevant in the cyberspace. This is because, the asymmetric nature of cyberattacks means that actors with limited financial and technical resources possess capability to compromise high-value targets (Masters, 2011). This logic can be extended to international relations to argue that even small or economically less developed countries may use the cyberspace to inflict harm to bigger and economically more developed countries.
The U.S. relationships with China and Russia in issues involving the cyberspace

The U.S. relationship with China involving cybersecurity

First it is worth noting that some cooperation between China and the U.S. has actually been achieved. In the early 2011, Chinese authorities and the U.S. FBI conducted joint operations to dismantle and shut down an illegal website dealing with child pornography (Lan, 2011). Despite the few instances of successful cooperation, allegations and counter-allegations have been persistent themes in dialogues and discourses in the U.S.-China relationships in cybersecurity.

Some Western analysts have also charged China for heavily employing freelance hacking groups in international cyberattacks providing “plausible deniability” about the state’s involvement. Western security analysts have maintained that although there is no definite proof, indirect and circumstantial evidence such as various digital fingerprints associated with the computer codes and the command and control computers and the malware products involved are too compelling to say that most of the high-profile China-originated cybercrimes are most probably associated with the Chinese government or the People’s Liberation Army (PLA) (Kshetri, 2013).

China is responding to the Western allegations by striking back with a strong denial and counter-allegation that U.S. government agencies lack interest in fighting cybercrimes and do not cooperate with their Chinese counterparts. Gu Jian, a vice-director of the Ministry of Public Security’s network security protection bureau, noted that China had received no response in its request for cooperation from the United States on 13 cybercrime cases involving issues such as fake bank websites and child pornography (China Daily, 2010). He further noted that in other cases it took up to six months to receive replies from the United States.
Chinese officials argue that they should be praised, not criticized, for their efforts to control cybercrimes at home and collaborate at the international level. They have pointed out that China’s active engagement in informal international relations have led to positive outcome (Kshetri, 2013). China has also warned against what it refers as a “blame game”. In a letter to the Financial Times’ editor, Dai Qingli, Spokesperson, Chinese Embassy in the U.K. 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” (Qingli, 2011).

Recent developments and events indicate that China and the U.S. are caught in the blame-counterblame cycle. Quoting to Chinese Internet insiders, a China Daily article on June 5, 2013 noted: “China has been the target of serious cyberattacks from the United States, but Beijing has never blamed Washington or the Pentagon because such accusations would be "technically irresponsible" …. The cyberattacks from the US have been as grave as the ones the US claims China has conducted” (Xiaokun, 2012).

The outcome is the lack of an extensive China-U.S. cooperation. Unlike the deep relationships of the U.S. with Estonia, Romania and Ukraine as noted earlier, the China-U.S. engagement in the cyberspace has been characterized by the lack of informal networks involving government officials from the two counties. For instance, if one country needs the help of the other country in investigating a cybercrime, a request for assistance takes place through an exchange of letters. It was reported that in 2010, the FBI office in Beijing forwarded 10 letters through the Ministry of Foreign Affairs and received responses to only two. This is in sharp contrast to the deeper and stronger collaborations and partnerships between the U.S. and EU countries. For instance, the Italy-based European Electronic Crimes Task Force, which has dedicated personnel from the countries involved to investigate and prosecute cybercrimes,
provides a forum for law enforcement agencies, the private sector, and academia from the U.S. and EU nations (Kshetri, 2013).

Especially following the Snowden leaks, China has expressed more hostile, sarcastic and furious comments towards the U.S. For example, a main heading in the front page of the overseas edition of the People’s Daily, the Chinese government said the alleged attacks by the U.S. on many networks in Hong Kong and China, including those of Tsinghua University, and Chinese mobile companies are matters of grave concern. The piece also noted that the Chinese government had taken the issue to the U.S. government (Elder and Kaiman, 2013). The newspaper praised Snowden for "tearing off Washington's sanctimonious mask". The newspaper went on to point out that the U.S. has gone from a “model of human rights” to “an eavesdropper on personal privacy” and an “invader of other countries' networks”. Global Times, which is closely tied to the CCP, observed: "Instead of apologising, Washington is showing off its muscle by attempting to control the whole situation" (Elder and Kaiman, 2013).

More specifically, the Chinese government suspects that it is under cyber-attack from the U.S. 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 (Adams, 2001). Chinese cryptographers reportedly found an “NSA Key” in Microsoft products, which was interpreted as related to the U.S. National Security Agency. The key allegedly provided the U.S. 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 U.S. government. Some U.S. 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 proposed sale of 16,000 desktop computers to the U.S. State Department. Due to the company’s connections to the Chinese government, politicians and some commentators drew attention to the potential national security implications of placing Chinese computers in U.S. government offices. Another Chinese high technology company, Huawei faced similar barriers in Australia, India, and the U.S.

**The U.S. relationship with Russia involving cybersecurity**

First it is important to consider actions involving some degree of cooperation between Russia and the West. In 2004, collaboration between British and Russian law enforcement agencies led to the arrests of members of an online extortion ring accused of blackmailing online sports betting websites that cost British companies US$120 million (sophos.com, 2004). In the mid-2000s, U.S. law enforcement officials reported receiving help from their Russian counterparts on about one out of six cybercrime-related requests (Bryan-Low, 2005). Russian cybersecurity agents were also trained in the U.S. (Swartz, 2008). Perhaps the most important sign of cooperation was Russia’s arrest of a St Petersburg-based hacker, Viktor Pleshchuk who was indicted by the U.S. for stealing US$9 million from the U.S. division of the Royal Bank of Scotland in 2006 (Moscaritolo, 2010). In June 2011, a Russian delegation led by the Russian National Security Council Deputy Secretary visited the U.S. and senior officials from the U.S. and Russia discussed cybersecurity issues facing the two countries (Schmidt, 2011).
Despite some progress in the past, the Russia-U.S. cooperation has been on ice for some time. U.S. law enforcement agencies think that their Russian counterparts’ responses to cybercrime-related cases are indifferent and uncooperative and see little or no value in working with them. In the Viktor Pleshchuk case, the U.S. government expressed dissatisfaction with Russia that he only received a six-year suspended sentence, which was low compared to U.S. standards (Moscaritolo, 2010).

Worse still, U.S. law enforcement agencies have perused Russian cybercriminals without notifying their Russian counterparts, which has created further conflict in the Russia-U.S. relationships. In 2000, the FBI arrested two Russian hackers by luring them to the U.S. with job offers. The FBI Agents handling the case also downloaded data from the two hackers’ computers located in Chelyabinsk, Russia. In 2002, Russia filed hacking charges against the FBI arguing that it was illegal to download data from computers physically located in Russia.

Likewise, when Vladimir Zdorovenin, a Russian citizen, was extradited to the U.S. by Swiss authorities for his alleged involvement in security frauds, computer hacking and ID theft in January 2012, Russian authorities complained that the Swiss and U.S. authorities did not notify them. A Russian Foreign Ministry spokesman commented: “Unfortunately, this is not the first time when US special services organize the detention of our nationals in third countries, often on dubious grounds and by provocative methods. What we’re looking at is the unlawful extraterritorial application of U.S. laws against Russian nationals” (RIA Novosti, 2012a). Likewise, in response to U.S.-based security researchers’ findings that a group of five men based in St Petersburg, Russia, was responsible for spreading the notorious Koobface worm, the Russian Embassy in the U.S. reacted that it had no information regarding that group. It further noted that U.S. law enforcement officials had never contacted the embassy about the group (Richmond, 2012).
As is the case of Zdorovenin, for the U.S., one way to pursue Russia-based cyber-fraudsters seems to be to arrest them when they travel to other countries that are allies. For instance, a Russian hacker, who was believed to attack Amazon.com and other U.S.-based e-retailers in 2008, was arrested in Cyprus in July 2012 (RIA Novosti, 2012b). He allegedly used botnet to attack Priceline.com and eBay systems as well, which requested resource-intensive pages from the companies’ systems and generated traffic, which was 600–1,000% of normal levels.

To move to a different issue, the Russian government’s responses need to be evaluated in the context of growing anti-Americanism in Russia (Shiraev and Zubok, 2000). Putin’s voter base consists of conservatives with anti-American feelings, values, attitudes and activities (economist.com, 2013). During most of the postwar period each side expressed open hostility towards the other (Lipson, 1991). It is argued that Putin has carefully cultivated and capitalized on the Soviet-era dogma of anti-Americanism (Shuster, 2013). In a state TV broadcast during his 2012 re-election campaign, he said: “I sometimes feel that America does not need allies. It needs vassals.” Unsurprisingly Putin’s foreign policy has clearly chosen not to be a U.S. vassal state (Shuster, 2013).

Although Russia and the U.S. have signed agreements in investigating some crimes, cybercrimes are not among them. In 2001, the U.S. Department of Justice (DoJ) requested the assistance from Russian authorities, but received no response (Lemos, 2001). Russia has also emphasized on international law to resolve cybercrime-related conflicts. A nice and striking example to illustrate this would be the example noted above, in which Russia in 2002 filed hacking charges against the FBI for downloading data from computers in Russia (Kshetri, 2010). Commenting on the orders of Putin and Obama to their security agencies to search for a way out
of the situation Nikolai Patrushev, the head of Russia’s presidential Security Council, said: “It’s not an easy task, because they need to find a solution in the framework of international law. There is no such norm, there is no … ready recipe” (Isachenkov, 2013).

The concept of isomorphism would help explain Putin’s approach to balance the interests of his voter base and the Western power. Isomorphism is positively related to legitimacy (Deephouse, 1996). Organizations able to acquire legitimacy from external actors are likely to gain resources as well as maintain control over the environment. Put differently, an organization can increase its chance of survival and/or growth by engaging in actions that are approved by powerful actors (Aldrich, 1999; Baum and Oliver, 1991; George et al., 2006; Meyer and Scott, 1983; Newman, 2000; Ruef and Scott, 1998; Sitkin and Sutcliffe, 1991). When actors with conflicting demands are to be appeased and served, however, a decoupling would help decision makers retain credibility and minimize cognitive dissonance (George et al., 2006). Different theoretical contributions and various empirical studies have led to the accepted view that exact nature of decoupling is a function of relative powers of competing institutional interests (March and Olsen, 1989; Oliver, 1991; Zajac and Westphal, 1995). These studies provide support for the notion that substantial responses cannot be made to appease actors opposing diametrically. The substantive response relates to the threat or opportunity associated with the more powerful actor (voter base) and the symbolic response relates to the threat or opportunity associated with the less powerful actor (Western power) (George et al., 2006). Putin’s spokesman told reporters that Russia has never handed anyone over and “won’t do so” and noted: “But neither Snowden nor anyone else should engage in anti-American activity. We hope that the situation won’t affect Russia-U.S. ties” (Runningen, 2013). Russia’s decision to grant Snowden temporary asylum (a
substantive response) and not allowing him to engage in anti-U.S. activities (a symbolic response) can be viewed as a decoupling of symbolic and substantive actions.

**Critical issues and areas of disagreement**

In order to understand the disagreements and conflicts associated with cybersecurity, it is important to note that prior researchers have placed an emphasis on multidimensionality of security and multiple forms of security risks (Tickner, 1994). Politicians and national elites in some countries have also underscored the importance of multi-dimensional aspect of cybersecurity. For instance, an article published in *China Economic Times* on June 12, 2000 discussed three mechanisms that Xu Guanhua, then Chinese vice minister of Science and Technology, thought high technology would affect 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”.

The importance placed on a given dimension of security significantly varies across time, space, issue area and according to specific political, geographic and cultural conditions. Critics of realism have claimed that it is insufficient simply to consider political and military issues as the only dimensions of national security (Tickner, 1994). Central to this perspective is a questioning of the traditional conceptualization of national security. For instance, developing economies have long emphasized the importance of economic threats in addition to military threats (Ball, 1988). Thomas (1987) viewed secure system of food, health, money and trade as the essential prerequisite to national security. Some researchers have also noted that threats to value and identity are important source of insecurity (Azar and Moon, 1988).
It is also important to distinguish between internal security and external security. When internal security poses a bigger threat, the defense against external attacks is likely to be a less important security goal (Tickner, 1994). Internal conflicts arise because social and economic and political systems work in the national elites’ advantage and they engage in exploitation of the majority of the people in the country (Tickner, 1994). Internal security is often desirable for the ruling elites to remain in power, which does not necessarily involve making all citizens equally secure and safe (Ball, 1988).

Cybersecurity also involves diverse dimensions and perspectives. At least three dimensions of cybersecurity need to be distinguished: military, espionage, and cybercrime. The emphasis of the U.S. has been mainly on controlling the last one: cybercrimes. Richard Clarke, the former U.S. National Coordinator for Security, Infrastructure Protection, and Counter-terrorism and Robert K. Knake, in their book (Clarke and Knake, 2010) have argued for a treaty that would ban cyberattacks on civilian targets but not on military targets or cyber exploitation. According to them, such a treaty would protect the private networks but would allow the lead it has in “cyber war against military targets” (p. 242). Clarke and Knake’s proposal does not intend to ban cyber-espionage. This is arguably because the U.S. relies heavily on electronic spying, and because verification of and attribution for espionage are too difficult in any event. The U.S. has repeatedly emphasized its interest in institutions that set the rules for controlling and punishing cyberattacks that involve economic espionage-related activities. The proposal is based on the premise that cyber espionage activities and military attacks are difficult to distinguish and one can be confused with the other. They oppose international legal regulation on this area because “an arms control agreement limiting cyber espionage is not clearly in [the United
States’ interest, might be violated regularly by other nations, and would pose significant compliance-enforcement problems” (Clarke and Knake, 2010, 236).

It is important to look at the approach taken by the Shanghai Cooperation Organization (SCO), which comprises China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan as its members. The SCO economies argue that they face different problems. These economies’ emphasis on the broader problem of “information security” rather than the narrower “cybersecurity” accounts for most of the major differences observed. In 2008, the 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 Western countries’ monopolization in ICT products such as software and hardware and less developed countries’ dependence on the West. In this way, they have emphasized on economic security, which was identified by prior researchers in conventional security threats facing developing countries (e.g., Ball, 1988; Thomas, 1987). A commentary published in the People’s Liberation Army Daily on 8 February 2000, without directly referring to any country noted that "some countries" with highly developed ICT industries are "taking advantage of their monopolistic position" to "control information technologies, infiltrate information resources" and dump IT products in underdeveloped countries. According to the article, the goal of these nations is "to attain political, economic and military objectives". Through the export of ICT products, the "information powers" dominate information in underdeveloped nations and thereby threaten their economic security.

A relatively high emphasis on internal security compared to external security, which prior researchers have observed in some countries (Ball, 1988; Tickner, 1994), can also be found in the SCO economies’ approach. They like to control information that is likely to provoke what
they call the three “evils” (terrorism, extremism, separatism). They also consider it important to prevent other nations from using their technologies to disrupt economic, social and political stability and national security. Western countries, on the other hand, maintain that too much government regulations and control may harm cyberspace security and emphasize the importance of the private sector in the formulation of international norms (Kizekova, 2012).

SCO states believe that the CoE Convention on Cybercrime fails to take into account a number of issues which is likely to lead to significant adverse impacts such as cybersecurity abuses and cyberconflict. Russia’s SCO National Coordinator Ambassador Barsky described the Convention as less than satisfactory (Kizekova, 2012). Russia has rejected the Convention arguing that it violates the country’s constitution by permitting foreign law enforcement agencies to conduct Internet searches inside its borders.

Regarding the military dimension of cybersecurity, the governments and national elites of China and Russia have viewpoints, which significantly complicate the international relations. Russia has placed heavy emphasis on the military dimensions of cybersecurity. Russia is arguably concerned about the U.S. superiority in the cyberspace (Andreas and Price, 2001; Maurer, 2011). It was reported that Russia and the U.S. had planned a dialogue which would include discussions about how each side’s military views the Internet and an effort to establish a hot line that could be used during cyber-security crises (Segal, 2012).

Two senior colonels of the Chinese military Qiao Liang and Wang Xiangsui in their 1999 book, Unrestricted Warfare, have argued that given the relative lack of resources of the PLA in conventional weapons, it should focus on the “development of new information and cyber war technologies and viruses to neutralize or erode an enemy’s political, economic and military information and command and control infrastructures”. The authors have forcefully argued that a
winning strategy would be to develop a means of challenging the U.S. through asymmetry rather than matching in terms of all types of resources.

Cyberspace is also linked to the threats to value and identity as source of insecurity as identified by prior researchers (Azar and Moon, 1988). As noted above, the problems of and concerns related to cultural securities have come to the surface recently. An article in China’s *People’s Liberation Army Daily* warned that the "information colonialism” is a real threat to national security, which “will be a major cause of future wars”. Due primarily to this concern, the Chinese government, has been building systems based on open-source software (OSS).

There is also disagreement regarding the appropriateness of certain venues for settling cyberspace related conflicts. While the U.S. has ratified the CoE convention on cybercrime, it has made very little use of this or other formal multilateral frameworks to resolve international conflicts involving the cyberspace. The U.S. considered the ITU and the ITRs as inappropriate international institutions for cybersecurity issues (Kramer, 2012). It is probably fair to say that compared to the U.S., China and Russia have made relatively more use of formal multilateral instruments to resolve cybersecurity-related conflicts and disputes. For instance, in September 2011, China, Russia, Tajikistan and Uzbekistan submitted a draft International Code of Conduct for Information Security to the 66th UN General Assembly Meeting. The code has called on nation states to “cooperate in … curbing dissemination of information which incites terrorism, secessionism, extremism or undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment”. Likewise, in the first meeting of the Intergovernmental Group of Experts of the UN Crime Prevention and Criminal Justice Program held in January 2011, the Chinese delegation, citing statistics of the China Ministry of Public Security, noted that in 2010, servers of over 90% of network sites that were used to commit
cyber-frauds such as phishing, pornography and Internet gambling against Chinese targets were located outside China. The delegation also stated that over 70% of botnet control sites were in foreign countries (Pi, 2011).

Let’s briefly look at the views of some of the U.S. national and political elites on the global cybersecurity problem. In a January 2010 speech on “Internet freedom”, U.S. Secretary of State Hillary Clinton noted: “Countries or individuals that engage in cyberattacks should face consequences and international condemnation. In an Internet-connected world, an attack on one nation’s networks can be an attack on all. And by reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons” (Clinton, 2010). In July 2012 General Keith Alexander, head of the U.S. National Security Agency and the Pentagon’s Cyber Command argued that IP thefts of U.S. organizations have resulted in the “greatest transfer of wealth in history”. He also estimated that the cost of IP theft to the US companies at US$250 billion a year (Joye, 2013). In February 2013, the U.S. government was reported to be considering fines and other trade penalties against a country guilty of cyberattacks (FoxNews.com, 2013).

Critics of the U.S. approach to international relations involving cybersecurity have listed several flaws. For instance, Goldsmith (2011) notes that “C&K’s [Clarke and Knake’s] proposal for a treaty that would benefit the United States and harm our major adversaries reflects a set of blinkered assumptions common in Washington discussions about the international dimensions of the cyber threat. … Until the United States gets serious about which concessions that are attractive to our adversaries it is willing and able to make, American talk of a cyber-arms agreement is empty”. Looking at Clarke and Knake’s proposal, General Alexander’s remarks and Clinton’s speech, the major barriers that may limit the U.S. success in international cybersecurity
cooperation may concern the assumption that the U.S. is merely a victim and not a part of the problem, and that U.S. activities are legitimate, while those of some major economies are not. Recent revelations regarding the NSA’s alleged engagement in spying activities that pursued a wide range of domestic and foreign targets including its allies and partners have further strengthened the critics’ point of view.

**The potential and the way forward**

Prior research has noted that similarity of members’ needs, clear boundaries, and shared norms and patterns of reciprocity are a key to effective cooperation (Bardhan, 1993). The above discussion indicates that most or all of these elements are largely absent from U.S.-China as well as U.S.-Russia relationships in cybersecurity. While the U.S. has successfully built informal institutions with some economies in some areas of cybersecurity, such institutions are largely absent with its engagements with China and Russia.

One way to analyze the behaviors of the relevant actors described above is to utilize economic game theory. Analyzing the interactions between European Parliament (EP) and the Council of Ministers, Farrell and Héritier (2003) suggested that such interactions can be treated as “infinitely repeated games”, which the actors view as linked to each other. An outcome of such interactions is that over time, the actors are likely to expect regularities in behavior. In this way, the bargaining processes among the game’s actors lead to informal norms (Farrell and Héritier, 2003). The game theoretic models predict a potentially large number of equilibrium outcomes in which observed past behavior of others may guide a player’s choice of actions. That is, even if the players face identical cost-benefit ratios, the degree of trust they have in each other would play a critical role in determining their actions. A breach of trust leads to a loss in reputation which would make difficult for the violator to persuade the others to “let bygones be bygones” (Seabright, 1990). In this context, as discussed earlier, the China-U.S. as well as
Russia-U.S. relationships are characterized by a low perceived trustworthiness. The game theoretic approach also predicts that if the players’ beliefs about each other’s trustworthiness are confirmed by subsequent behavior, there is a tendency of cooperative behavior to enhance the prospects for successful further cooperation (Seabright, 1990). In the absence of trust-building measures, it would be unrealistic to expect that China and Russia would engage in cooperative behaviors in the cyberspace.

At the same time, as noted above, the U.S. is moving away from formal treaties. Given the lack of preference and success of the U.S. in building formal institutions involving the cyberspace with key economies, its success in the engagement in international relations involving the cyberspace hinges critically upon the formation of successful informal institutions. In this regard, whereas prior researchers have identified informal institutions’ vital roles in security relationships and other outcomes (Farrell and Héritier, 2003; Lipson, 1991), such agreements have even more critical roles to play in resolving cyber-conflicts.

The next natural question to ask is how such institutions can be built. Farrell and Héritier (2003) suggested that the nature of cooperative activities and repeated interactions among actors lead to the formation of informal institutions. In prior theoretical and empirical research, psychologists and economists have found that the norm of fairness in the interactions would guide the actions of most actors (Bardhan, 1993). That is, in most cases, people do not want to free ride on others’ cooperation and they are not willing to cooperate when others do not. To put things in context, the past history of cooperation and conflicts between nations should be taken into account to understand international cooperation on cybersecurity. In this regard, suspicion, accusations and lack of cooperation as noted earlier indicate the lack of and deteriorating trust with key global economies.
As a related point, commenting on the limitation of prisoners’ dilemma game theory, Sen (1987) noted that in order to understand the behavior patterns of the members, it is important to go beyond mutual interdependence and emphasize on “self-goal choice” and enhancement of the respective goals of the members. Thus, discussions about formal and informal international institutions should also recognize the different goals and objectives of other countries. In this regard, a drawback of Clarke and Knake’s (2010) proposal is that it is meant to serve the goals of the U.S. and makes little or no attempt to consider many other countries’ viewpoints, perspectives, positions, and standpoints. Such a treaty obviously has a relatively low chance of success.

At a hearing of the House Foreign Affairs subcommittee on Asia, James Andrew Lewis, Director and Senior Fellow, Technology and Public Policy Program and director of the technology program at the Center for Strategic and International Studies noted: “We need to persuade the Chinese to change their behavior; we can’t coerce them, they’re too big. There are factions within China that want to work with us. We need to encourage them” (Freedberg, 2013). One way to build more effective informal institutions would be to lean toward a “softer” approach. It was reported that the Subcommittee chairman, Steve Chabot was willing to adopt a soft strategy. Likewise, while the Chinese leftist leaders and some government officials associate China’s global integration with significant socioeconomic costs, there are factions within the CCP that consider integration with the world desirable and important.

Analysts argue that the fact that China’s “post-Tiananmen generation” has experienced little or no hardship has made this generation indifferent to democracy (Hvistendahl, 2009). Chinese society is conditionally tolerant of the domination of civil society by a strong state. Thanks to China’s Internet-driven nationalism, however, opposition to the West has become one
of the defining values of this generation. This means that Chinese politicians are in a position to acquire a huge number of supporters on the home front by engaging in anti-west activities involving the cyberspace. On the other hand, global integration is a matter of central importance for many liberal CCP leaders and the Chinese government. This means that it may be possible to work with China to address some of the major conflicts involving the cyberspace.

**Discussion and implications**

The rapid technological evolution means that there is a wide variety of choices available to implement in cyber-offense and cyber-defense activities. In order to illustrate this point, let us consider the following statistics. According to IBM, 2.5 quintillion (250,000,000,000,000,000) bytes of data is created every day. IBM also estimates that 90% of the data in the world today has been created in the last two years (ibm.com, 2013). The examples discussed above such as Stuxnet virus to damage Iran's centrifuges at Natanz nuclear site (Rid, 2012) and cyberattacks on the Office of the Dalai Lama indicate that the Information Age has offered some distinctive advantages to governments to fight or make headway against their adversaries. At the same time in theory and empirical research, scholars have shown that digital weapons can be and are being used to target and destroy nations that rely on digital technologies (Cobb, 1999). It is also more difficult to assess an adversary's cyber-capabilities since such capabilities are developed more recently. In the digital age, it is thus difficult to predict who the decisive winner would be (Simmons, 2011).

Compared to the rapid development in ICTs, formal and informal institutions related to cybersecurity, both at the national and international levels, have been slower to change. As the above discussion makes it clear, there are deep and fundamental clashes regarding the nature of
the problem, the practices that should be outlawed and the appropriate venues and mechanisms for settling cybersecurity-related international disputes.

The existence of reputation mechanisms and multiplex relationships, which involve relationships based on more than one set of roles make sanctions easier to apply (Bardhan, 1993). For instance, Russia is reported to make some progress to become an OECD member. If Russia gains an OECD membership, its engagement in cybersecurity-related international cooperation can be expected to improve.

Prior researchers have suggested that organizations tend to change structures when confronted with ambiguity and poor performance (Newman, 2000). These are reflected in the PLA’s intention and preference to develop information and cyber war technologies and the NSA’s development of the massive surveillance programs. For instance, the U.S. realized that institutional weaknesses contributed to poor performance in areas related to national security, which led to the formation of new institutions to enhance cybersecurity. Such changes may create confusion and uncertainty and produce an environment that lacks norms, templates, and models about appropriate strategies, structures, and legitimacy (Greenwood and Hinings, 1993; Newman, 2000). Prior research also indicates that it is difficult to learn from experience during periods of significant institutional change, because past experience is no longer an appropriate guide for future actions (Weick, 1979). Recent cyber-conflicts have provoked a high degree of confusion and conflict among nations.

We can also draw insights by comparing the current U.S.-Russia relationship with the U.S.-Soviet relationship during the Cold War era. As is the current situation, the U.S. and the Soviet Union had made very few direct treaties and even fewer in key areas related to national security (Lipson, 1991). Nonetheless the two economies’ engagement was governed by tacit
relationships developed over time. In this regard, the really big difference between the current and the Cold War era situation is that there has been a lack of tacit understanding to guide the relationship governing the cyberspace.

Prior research suggests that some nations may consider their behaviors justifiable or excusable if others have already violated the agreement (Lipson, 1991). In this regard, China and Russia may think that the U.S. might have already violated such “tacit” agreements involving the cyberspace. Changes in circumstances and the lack of feasibility in compliance may also change nations’ response to behaviors (Lipson, 1991). As noted earlier, following the Snowden leaks, China saw that it gained an upper hand on the issue and expressed more hostile comments towards the U.S.

**Directions for future research**

Cybersecurity related concerns have led to various barriers to international trade and investment in a broad range of countries. For instance, Australian, Indian, and the U.S. governments have accused the Chinese company, Huawei Technologies of cyber-espionage, which hindered the growth of the company’s businesses. Likewise, Chinese, Russian, and the U.K. governments have expressed national security concerns about Microsoft products. In future conceptual and empirical work scholars need to compare and contrast the processes involved in the impacts of such concerns on international relations and on international trade and investment politics.

It is also important to see international relations related to cybersecurity in the backdrop of relationships in other areas rather than as a self-contained phenomenon with self-contained solutions. Put differently, the present aspects of U.S.-China and U.S.-Russia relationships related to cybersecurity are, to some extent, the results of the past relationships. In this regard, future researcher may provide new insights on issues related to the cybersecurity-international relations nexus by systematically examining relationships among nations that have more similar interests.
and comparing with such relations among economies characterized by hostile relationships such as those examined in this paper.

Our study mainly focused on international relations among geopolitically significant economies. The effects of cybersecurity-related factors on international relations among smaller economies might be worthwhile target of study.

Finally, countries’ cybersecurity-related behaviors may trigger reactions from actors in the firm’s nonmarket environment such as interest groups, the intelligentsia, and public opinion, which may provide a possible mechanism, which may shape international relations among economies. Another area of exploration would be how the various non-market forces affect cybersecurity-related international relations among countries.

**Concluding remarks**

International relations involving cybersecurity is at an infant phase of institutionalization and presently undergoing an evolutionary trend, which is likely to lead to fundamental and rapid institutional changes. A problems hindering efforts to develop international cooperation is that nations have exhibited a tendency to consider only their internal needs and preferences and disregard other nations’ perspectives and viewpoints. For instance, they are still far from consensus on key issues such as the appropriate venues for cybersecurity related formal agreements and the roles of the governments and the private sector on Internet governance. There has been the lack of tacit relationships or moral agreements regarding nations’ engagement in the cyberspace. Likewise, people involved in law enforcement in major economies tend to view their counterparts in other countries with suspicion and animosity and their expectations often orient around distrust and conflict.
The U.S. has encountered a wide range of barriers to developing an informal cooperation with key economies. Despite some sign of cooperation, the Russia-U.S. relationship on the cybersecurity front is not friendly cooperation but mostly intense distrust and even hostility. A similar point can be made about relationship with China. The poor track record of the U.S. in dealing with cybersecurity issues associated with China and Russia can be attributed in large part to the fact that, its relationships with these countries are characterized by lower levels of integration and weak and ineffective informal institutions. The Snowden case is an indication that China-U.S. and Russia-U.S. relationships are at deteriorating rather than developing stages in terms of cybersecurity. Russia granted him asylum despite fierce protest from and to the discomfort of the U.S. government. These governments have failed to engage in substantive cooperation on a variety of issues that are increasingly important for global cybersecurity.

The U.S. has negotiated no formal treaties with China or Russia and has been slow to develop informal cooperation and non-treaty-based relationships. The presumption that the U.S. is an innocent victim but not a part of the global cybersecurity problem seems to pervade the contemporary U.S. policy discourse. In this regard, it is important to keep one overriding reality in mind: the U.S.’s alleged involvement in activities such as the creation and launch of Stuxnet virus and the hacking of Brazil’s state-owned Petrobras oil company's networks means that other economies widely perceive that the U.S. has violated the codes or rules to engage in the cyberspace. Ironically, the truth or falsity of the allegation is less relevant than the fear itself, which can significantly alter the perspectives on cybersecurity-related international engagements.

Prior research indicates that progressive institutional changes are sustainable only if there is a “minimal dislocation” (Bush, 1994). Given that the U.S. has significant disagreements on cybersecurity with Russia and China, it is unreasonable to assume that a single approach can
possibly address all the cyber-conflicts. To develop more effective cooperation with these countries need to identify areas of mutual interest (e.g., help develop the legitimate Russian IT industry which would employ the IT manpower and stop them from pursuing a cybercrime-related career) and collaboration and engage in confidence building and security cooperation. It is important to avoid areas that they disagree quite sharply and fundamentally.
References


Khalil, A. 2012. 89 ITU members sign controversial UN telecom treaty. Available at <http://www.google.com/hostednews/afp/article/ALeqM5gDVKYraZhijiirU7PP0ILa568zi3Q?docId=CNG.a05a10530f905edbf666f144293e18f_3d1>. Accessed 16 September 2013.


Pi, Yong. 2011. New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime, Shared with the Council of Europe for publication


Swartz, J. 2008. Cybercriminals can’t get away with it like they used to USA Today.


