Cybersecurity-related international institutions: An assessment and a framework for nations? strategic policy choices

- Area: ROADMAP FOR THE FURTHER EVOLUTION OF THE INTERNET GOVERNANCE ECOSYSTEM
- Entitled by: Nir Kshetri
- Region: USA
- Organization: University of North Carolina-- Greensboro
- Sector: Academia
- Keywords: Cybersecurity, international institutional frameworks, informal agreements, diplomatic and economic ties

Abstract

The presentation provides a review of initiatives and measures introduced by the Council of Europe Convention on Cybercrime and other international/regional organizations and relevant bodies and fora for reducing cyber-threats. It argues that the current legal regimes, institutional frameworks and instruments are insufficient, inappropriate and ineffective to address cyber-threats. I propose a number options to engage with nations such as contributing to local capacity building and institutional development, creating informal networks and agreements, providing opportunities for developing economies? voice and participation, harnessing the power of regional organizations, achieving cooperation on common areas of interest, helping develop the local ICT industry to absorb manpower that would otherwise venture into criminal world, encouraging integration with the West, establishing high level working groups and developing offensive and defensive capabilities tailored to specific threats.

Document

A framework for nations' strategic policy choices for cyber-conflicts associated with various sources

Table 1 here

Theoretically, the international institutional framework for cybersecurity is structurally

imperfect and deficient from an industrial country's perspective. Based on the above discussion, the relationships among countries from the perspective of cybersecurity-related relationships can be divided into four groups that pose different dominant challenges when viewed from a Western country's perspective (Table 1).

Local capacity building in law enforcement and institutional development

Some emerging economies' law enforcement system capacity to deal with cybercrime has become the dominant challenge that limits their ability to fight cybercrimes. EBay'sAlbena

Spasova, who worked in promoting law reform in Moldova and Bulgaria noted: "Even in 2001, I was meeting judges who thought cyber-crime was someone stealing a computer" (Wylie, 2007). Local capacity building and institutional development can produce effective results in strengthening global cybersecurity. As an example, consider Romania.As of 2013, the U.S. Federal Bureau of Investigation (FBI) trained about 600 Romanian investigators in fighting cybercrime (Odobescu, 2014). Some affected private sector players have also contributed to promote institutional and law enforcement capacity development. To take an example, eBay has been educating Romanian prosecutors about cybercrimes including explaining to a judge using layman's language (Wylie, 2007). In response to the rise of Romania-originated cybercrimes, the Council of Europe selected the capital city Bucharest for its latest cybercrime program office.

Creation of informal networks and agreements

Trans-governmental informal networks consisting of regulators and public officials are becoming an increasingly common feature of global governance(Bach and Newman, 2010). Such networks exist in areas such as financial markets, aviation, antitrust, data privacy, pharmaceuticals, and environment (Bach, 2010; Newman, 2008). Officials from many countries work together to share information, develop harmonized guidelines and best practices, and reduce frictions.

Since 2009, the FBI permanently based a cybercrime expert in Estonia. The FBI worked closely with the Estonian Police and Border Guard, which led to the *arrest of six Estonians* , who allegedly hijacked over 4 million computers in over 100 countries and illegally made at least US$ 14 million (Kshetri, 2013b). Since 2009, the FBI has also stationed a special agent at the U.S. Embassy in Kiev. In 2010, the SBU arrested five alleged kingpins of a criminal group, which stole US$ 70 million from U.S. bank accounts (Onyshkiv and Bondarev, 2012).

On the contrary, the systems used by China and the U.S.*are inefficient*. If one country needs the help of the other, a request for assistance takes place through an exchange of letters. In 2010, the FBI office in Beijing reportedly forwarded 10 letters through the Ministry of Foreign Affairs and received responses to two. This is in sharp contrast to the deeper and stronger collaborations and partnerships between the U.S. and EU countries.

For instance, the 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.

Providing opportunities for developing economies' voice and participation

Treaties involving alliances and broad policy guidelines are sustained only by perceptions of mutual advantage (*Baxter,* 1980). Making efforts to understand developing economies' problems from their point of view and providing opportunities for their voice and participation would help explore mutual advantage and encourage their participation in formal international frameworks. Attempting to achieve too much too rapidly is often counterproductive. One way to gain their cooperation would be exclude issues from formal treaties that are objected by developing countries and are only tangentially related to cybercrime such as software piracy.

Establishment of a high level working group made up of policy makers

External pressures can do little to force nations to change their cyberspace behaviors since outsiders lack broad legitimacy. In order to find a solution that satisfies both parties, it is important to engage policy makers and national elites with strong commitment to a soft approach to and interested in developing a *better relationship with adversaries*. We illustrate this with the following observation involving China-U.S. relationships in cyberspace.

At a hearing of the U.S. House Foreign Affairs subcommittee on Asia, the 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 is to use a soft approach. It was reported that the Subcommittee chairman, Steve Chabot was willing to adopt a soft strategy. Likewise, there are *factions within the Chinese Communist Party (CCP) that consider integration with the world desirable.* Like-minded policy makers from both countries who prefer soft approach and seek to ameliorate the root causes of cyber-threats through negotiation, conciliation and compromise can help incrementally develop formal and informal relationships.

A 'bricolage' approach to cybersecurity

The different approaches to protect against cybercrimes discussed earlier do not directly deal with the fundamental sources of the problem. For instance, for most former Soviet Union economies, the basic source of the problem can be traced to the fact that most of them are too small to absorb the existing computer talent (Serio and Gorkin, 2003). A self-described hacker from Moscow noted: “Hacking is one of the few good jobs left here” (Walker, 2004).

In this regard, combining components from the existing institutions and reorganizing strategically—or bricolage—can be an important way to enhance cooperation (Campbell, 2004). For instance, Western companies can work closely with governments to *help develop the ICT* industry would help address the concerns regarding the West’s monopolization in ICT products.

Identifying and achieving cooperation on common areas of interest

Identifying and achieving cooperation on common areas of interest may help secure a "foot-in-the-door" for a subsequent more significant collaboration. To take an example, i n 2011, Chinese authorities and the FBI conducted joint operations to shut down a child pornography website (Lan, 2011). The Chinese government has thus taken at least symbolic actions to collaborate with the U.S. Theorists argue that a symbolic action may lead to more substantive actions subsequently (Campbell, 2004).

Helping, encouraging and providing incentives to integrate with the West

Cybercriminals can take advantage of jurisdictional arbitrage by operating from economies with outdated legislative framework and the lack of *law enforcement* system capacity. They can do so even more effectively by operating from economies with a low degree of cooperation and integration with the West. *E*merging economies’ deeper integration with the West would force them modernize legislative frameworks and enhance system capacity and law enforcement.

A related point is that multiplex relationships make sanctions effective (Bardhan, 1993). For instance, Russia is making progress to join the Organization for Economic Cooperation and Development (*OECD*). If Russia gains an OECD membership, it may experience additional pressures associated with the membership and its engagement in cybersecurity-related cooperation may improve.

Harnessing the power of successful regional organizations

One way to compensate some of the deficiencies of the existing cybersecurity-related international institutions is to harness the power of regional organizations, especially consisting of developing nations that are not signatories to the CoECoC. Successful regional organizations that are internally cohesive and have *security as a key focus* are logical candidates. The ASEAN is one example that fits these criteria and has been

effective in managing its internal security relations *(Narine,*1998). Some economies' engagement with the ASEAN has focused on cybersecurity. Since 2009, the ASEAN and Japan have collaborated on cybersecurity. Relevant ministries and agencies such as Computer Security Incident Response Teams (CSIRTs) of ASEAN Members and Japan have focused on initiatives such as Internet Traffic Monitoring Data Sharing (TSUBAME) Project (http://tinyurl.com/p44yx82). Likewise, in July 2013, a U.S. delegation participated at the 20th Meeting of the ASEAN Regional Forum (ARF) in Brunei Darussalam. Cybersecurity is one of the four core areas addressed by the ARF within its work on counterterrorism and transnational crime (http://tinyurl.com/m4vedhb).

***Offensive and defensivecapabilities*tailored to specific threats**

The responses discussed thus far are appropriate only if the sources of cyber-attacks have formal diplomatic and economic ties. In the absence of such ties, cybersecurity may require a balance of *offensive and defensivecapabilities.* Proactive defense tailored to specific threats is important. For instance, in response to North Korea-originated GPS attacks, South Korea is developing advanced GPS technologies.