COOPERATION MODEL BETWEEN MULTIPLE SECTORS: BRIDGING BETWEEN GOVERNMENTS, INDUSTRIES AND LAW ENFORCEMENT

PAPER TITLED : COOPERATION MODELS AND COMPELLING ISSUES AMONGST PARTICIPATING PARTIES

SPEAKER NAME : DATIN AISAH ZAINAB MAHMUD, JAGAT TECHNOLOGY

25th_Mahmud.ppt

AGENDA

- Issues and Challenges for the Governments in Cyberspace
- Mechanisms for Regional Cooperation in combating computer crimes
- Regional Developments that have been taken so far
- Cooperation among industries and law enforcement

What is Cyberspace?

- Cyberspace is-the Internet and other computer-based networks.

  Its main characteristics:

- Computer connected through standartized code of protocol;
- It is borderless;
- Difficult to control

Challenges for governments in Cyberspace

- The laws dealing with computer crimes are not harmonized, makes it difficult to enforce law; clear example, “I love You” virus which was released in Philippine and at that time (2000) the country did not have legislation to address cyber crimes.
- Extradition procedures, which can hinder the works of law enforcement officers
- Some countries (especially developing countries) do not have experts in computer crimes;
- There is no established center for information sharing in this region;

Ways to Address

- Standardization: this involves creation of environment for development of standard protocols, applications, workstations and server configurations;
- Information sharing among governments' relevant agencies;
- Legal coordination and providing (developed countries) aid to developing countries in training, funding etc:

Model for Inter-governmental cooperation should include these:

- All cooperating countries would share a common baseline perception of what constitute “criminal behavior” in cyberspace;
- Each of the governments of the region should have substantial confidence to deal with the problem of preventing and punishing attacks on cyber systems.
- There must be capabilities and policies to provide effective security within each government’s jurisdiction;
- Each country should have substantial capability in active, preventive defense, and competent national authority for engaging in active defense;

- International responses to transnational attacks would be covered under regional-umbrella convention that will permit timely action under established procedure;

  This would include the need for legal and administrative policies in order to create a framework for regional interaction, including setting well-defined boundaries for legal actions or possibly creation of multilateral treaty;

Developments

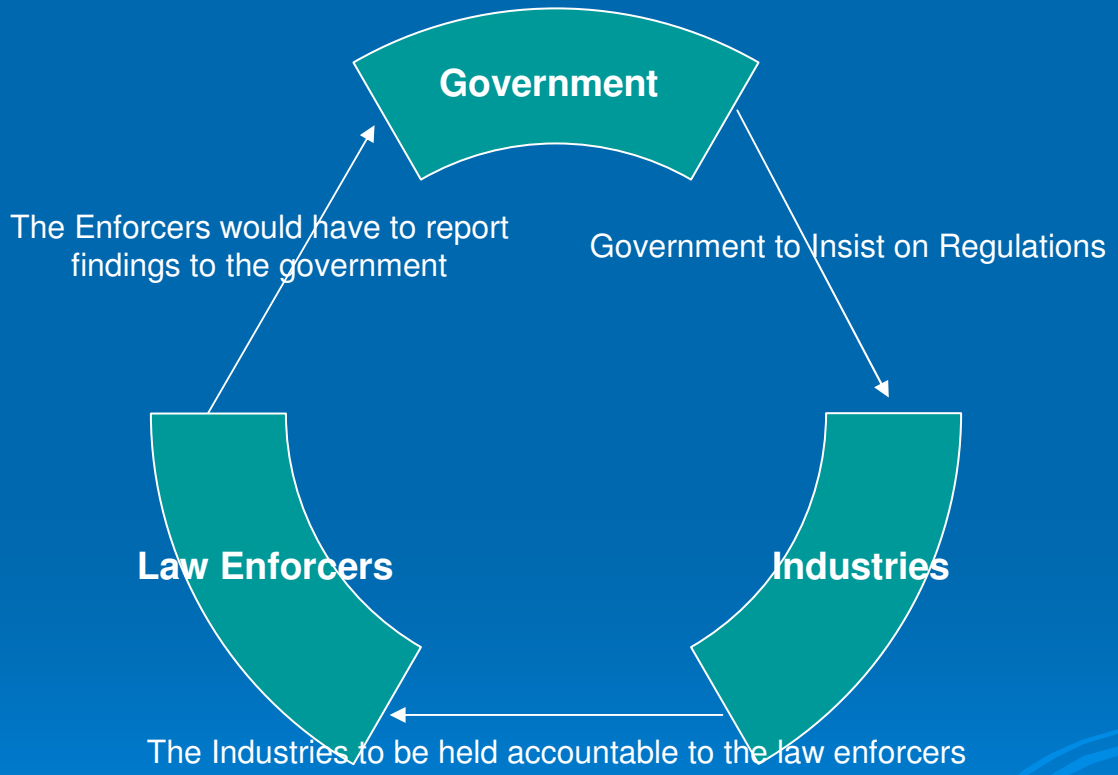
- EU they have adopted Cyber Crime Convention in 2001, which is open for all countries;
- It requires member-countries to harmonize their legislations on computer crimes to the standard of the Convention;
- Laid down procedures for cooperation among law enforcement officers amongst member-countries;
- Agrees to set-up 24/7 center for information-sharing among member-countries; (Article 35)
- Providing funding for training of personnel involved in cyber crime investigation;
- So far 33 nations have signed the Treaty, including USA, Canada, Japan, UK and other European nations. (Cont'd)

- It will come into force, when 5 nations ratify it including 3 member-states of EU.
- So far 4 nations have ratified the Treaty.
- Organization of Americas States: Meetings of Minister of Justices or Attorney Generals' of Americas (REJMA) in their meeting made recommendations on the number of subjects relating to law enforcements, cooperation and training on information security on June 23, 2003

Recommendations

- Ultimate aim would be for the Global Treaty. However as the first step, countries should adopt regional or bilateral arrangement to enhance cooperation;
- Harmonize their respective legislations and procedures for extraditions;
- Countries in ASEAN should consider adopting mutual assistance treaty to facilitate law enforcements and training;

The relationship between Government, Industries and the Law enforcers



Apart from the understanding between Government, Treaties, there is a need to educate the Industries in Order for them to protect their Information as well

The Role Model for such Industries would be as such:-

- The Industries should be encourage towards the creation of a "culture of security compliance" across all sectors.
- The industry should develop online programmes with the task of educating users as well as workers on the importance of developing a Safe Network Environment.
- Business enterprises and governments are expected to collaborate both internationally and locally in order to protect the Internet from external attacks. Developing countries and economies are to work towards the creation of regulatory measures that would ensure minimum standards of protection for confidential information, security of networks, and security of transactions.

- The corporations are to develop business processes for security management and establish a security management system, operated and initiated by senior management.

- There must be a Security Policy, which clearly states the position and basic understanding of the corporation regarding information security, for example, how to protect information and data inside its own information network and system, should be established. Security Program including business continuity in emergency situation would be also effective.

- A need for the appointment of Chief Information Security Officer, who would be responsible for information security at all levels, may be appointed. He/She should be responsible for ensuring policy consistency, clearly defining policies, identifying and consistently enforcing consequences for non-compliance, and instituting a governance framework to monitor and control the execution of processes and procedures.

- The Systems, networks and policies of corporations would need to be properly designed, implemented and coordinated to optimize cyber security. Cyber security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. The Government should set a Basic standard in the Regulating such a System. Corporations should respect and implement this principle not only as a provider of services and devices for information systems but also as an owner or operator of its own information systems and network.

- All participants and stakeholders of the Internet and e-commerce should be aware of the need for security of information systems and networks and what they can do to enhance security. Awareness of the risks and available safeguards is the first line of defense. Information systems and networks can spread harm to others as a result of interconnectivity and interdependency.

- Risk assessment of information systems and networks should be conducted and the results shared in global cases. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to include key internal and external factors, such as technology, physical and human factors, policies and third party services with security implications

There is a need to insist on the usage of the code of Best practices for an ICT-related investment or other commercial activity with the emphasis on the following issues:

- *Sustainability*: the viability over time of a commercial activity, including the prospect of a long-term return internally generated by the activity;
- *Appropriate technology*: the choice of an ICT technology adapted for the market within a developing country that is suitable within geographic and environment constraints, targeted for skill-sets and objectives of users, to ensure take-up of the technology and commercial return;
- *Local contents*: software or other contents, developed in the target country or region, to be included in the product or service offered, both as a tool to meet local market characteristics and also to bring local partners into its development.

- Public authorities should be aware of the business decision process undertaken and the criteria applied by a company when deciding on a commercial activity Industry is encouraged to continue, in emerging economies, its activities and training efforts as a complement

- There is also a need for the change of the laws to accommodate the changes on the Cyber World. Due to jurisdictional issues, a cyber crime can be committed from any where of the world. And as a result, one would be at stake when talking about apprehending a suspect out of jurisdiction.

- With regards to the enforcement by the public bodies, one has to realize that there is a need to set fixed standards against industries and the local public bodies would need to ensure that the companies accommodate the suggestions e.g. code of Best Practice

- Security management systems and programs should be established and operated effectively. They should be based on risk assessment and should be dynamic, encompassing all levels of corporate activity and all aspects of corporate operations, and be initiated under the leadership of the CEO or a senior appropriate executive”””. Information system and network security policies, practices, measures and procedures should be co-oriented and integrated by security management to create a coherent system of security.

- The need for the Promotion and required interoperability of digital signature and public key infrastructure, which are bases for global electronic commerce. Importance of information sharing between private sectors and governmental sectors on cyber crimes law enforcement agencies expect the owner of information systems under external attack to report any damage and request that the ISP or other private operators disclose the access logs or communication logs both industry and governments create a reporting system that would collect all the cases found, and that industry undertake to report all the attacks.

- The Importance for senior management to ensure that their networks can support business continuity and profitability objectives should be viewed and regulated.

- The need of the Government to insist on Certification and security standard

Why the need for such a Model?

- In 1999, the Authentication and Security Working Group made a recommendation which focused on developing key principles including “Protection” and “Promotion”.

- **European Cyber Crime Convention -** In November 2001, the Council of Europe adopted the Convention on Cyber Crime. In order to fight cyber crime, there is a need to clarify what constitutes an offence or a crime, especially when we speak about a global scenario where definitions of illegal activities pursued worldwide are needed. Governments should agree on the definitions of certain crimes committed in the Internet environment.

  There are other crimes like money laundering, fraud, denial of services, spread of viruses and other related activities that should be agreed upon and condemned and treated as crimes on the internet.

- **Increasing damage by viruses and cyber attacks -** The more people use the Internet, the greater the chance for increased cyber attacks and viruses. In East Asia, for example, always-on access to the Internet by Digital Subscriber Line (DSL) has multiplied the number of computers and information systems damaged by viruses and cyber attacks because many computers and systems are not sufficiently protected to face being connected to the Internet 24 hours a day, seven days a week. A similar situation may also occur in other areas outside of Asia (e.g., Eastern Europe, Africa, and Latin America), where the use of the Internet by DSL is expected to grow in the coming years.

Culture of Security

- With respect to the new trends in cyber security, governments and international organizations have made further efforts to promote cyber security policies. Governmental concern has focused on a number of issues including combating and preventing cyber crimes, protecting critical infrastructure against cyber attacks and improving the security of government information systems. These legal and legislative activities have come to be discussed globally and therefore, international harmonization is also being considered.

- In addition, many government initiatives for promoting Information and Communication Technology also mention cyber security as one of the top priority issues. For example, “e-Europe 2005” states that the private sector should develop good practices and standards and promote their consistent application in the context of “culture of security”6. The “e-Japan Priority Policy Program 2002” emphasizes “ensuring the security and reliability of the advanced information and telecommunications network” as one of priority policies, which recognizes the role of industry as important to some extent.

- Government activities in cyber security have reached a new phase of development with the initiation of international business discussions to begin combating cross-border cyber crime. The private sector has also been involved in dialogues to investigate new methods and ideas in cyber security.

- Governments of the Organization for Economic Co-operation and Development (OECD) have drawn up new Guidelines for the Security of Information Systems and Networks. These guidelines are designed to develop a “culture of security” among government, business and users in an environment of worldwide expansion of communications network, increasing interconnectivity across national borders, converging technologies and ever more powerful personal computers.

- It is expected that the Internet will expand much more in all regions of the world with all kinds of users and that all generations will join the Information Society through the Internet. In such a situation, cyber security should be established as a significant part of information infrastructure worldwide. Cyber security should be implemented in a manner consistent with the values recognized by democratic societies, which include the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency. To realize cyber security, all stakeholders of the Internet (governments, industries, academics, and personal users) should be aware of the need for information security and what they can do to enhance it.

- They are responsible for the security of information systems and networks, and, therefore, should be accountable in an appropriate manner depending on their individual roles. For example, governments should establish legal and regulatory frameworks for public security, and provide secured information infrastructure as public services. Industries should not only develop and invent more secure technology for information and communication, but also adopt a comprehensive approach to security management.

The need for security is inclusive of the following

- **National Security**
- **Public Security**
- **Security for industries**

National Security

- Combating cyber terrorism, protecting critical infrastructure against viruses and cyber attacks, national espionage, and related issues are a high priority for governments. Governments should take active initiatives on these matters taking into account the interests of industry. Industry should, in turn, cooperate with governments to find the best solution. The solution should not result in increased burden or the imposition of higher costs for business development.

- One has to recognized that the military defense is one that would have a direct risk to National Security in the event that there is a successful hacker as the Military Information could be easily be used against the said country. This is a credible threat as the Defenses available may be not sufficiently sophisticated.

Public Security

- Cross border cooperation between law enforcement and international legal infrastructure for combating cyber crimes is crucial in making progress on this issue. Also for this kind of issue, governments should take initiative for settlement and industries should support government initiatives, which do not present an obstacle to business development.

Security for industries

- There are many cyber security issues which companies should make efforts to resolve; for example, protecting information systems or enforcing security policy for security management among others. This kind of issue should be called “security for industries” and governments are expected to support such industrial activity and effective efforts.

Elements to be Considered

- **Security & the Business Enterprise**

  Information Security is a crucial issue for business enterprises. Businesses need to protect information systems from external and internal attacks as key elements in their business operation; their activities are exposed to the risk of being damaged by possible attacks on critical social infrastructure, as the world becomes more and more dependent on broadband Internet access. These issues are important in terms of risk management, and directors and senior management need to be clearly informed about these issues.

- Therefore, industry should encourage the creation of a "culture of security compliance" across all sectors. Most users are not aware of the extent of damage a single virus could cause both in economic terms and by harming infrastructure. Also, an employee acting without due diligence in his/her job could cause the same harm as if he/she had intentionally launched an attack against certain infrastructure.

Collaboration & Internet Protection

Business enterprises and governments are expected to collaborate both internationally and locally in order to protect the Internet from external attacks. Specific goals include the promotion of voluntary information sharing on cyber crimes and cyber attacks within industry, with the assistance of governments, and the close cooperation of industry with investigation authorities on various responses to cyber crimes. At the same time, it is important to limit the burden on industry in cooperating with investigation authorities.

- **Lack of Funds & Security**

  Attacks against information systems are one of the major obstacles hindering the development of electronic commerce and the Internet. These activities not only harm consumer confidence in the use of the networks as a new tool for business, but also impose an economic burden on the private sector and on the public bodies and consumers, which threatens to make information systems more costly and less affordable for users.

  The issue of security is fundamental when seeking a good implementation of information society services in developing countries. Experience in developed countries has shown that consumers are reluctant to use electronic commerce if the network is not reliable enough to protect electronic transactions or the transfer of confidential information. Thus, a secured network is more reliable for users and consumers.

  Therefore, to achieve the rapid implementation and use of electronic commerce in developing countries, it is necessary to take proper measures regarding the protection of personal data, secure electronic transactions and security of networks.

What is Certification and security standard?

In order to enhance the quality of information network security - standardization of response measures, risk assessment, and security management, enhanced by education and promotion - it is essential to focus on security measures themselves. Higher perception of information security by network providers, individual users or SMEs improves the quality of security throughout the network and makes it less susceptible to viruses and cyber attacks.

There exist as many methods of security management and certification as providers of management and certifications. While they take different approaches, they are effective and successful insofar as they are recognized and accepted by customers depending on tastes. However, such management and certification should be operated and adopted by both governments and industries on global basis.

Such risk assessment and risk management should include forward-looking responses to emerging and potential threats to information systems and networks.

Information sharing/collaboration

Various international conferences have also discussed the importance of information sharing.

Information sharing is discussed in the context of protection of information systems from the “attacks to critical infrastructure” at its initiation.

In the context of reacting against terrorism and other attacks and other business disruptions, Governments have already started discussions regarding the critical infrastructure at the nation’s base, and in many cases they have implemented best practices.

Other information sharing between public and private sectors on virus attacks or denial-of service attacks should be discussed in a separate context from the attacks to critical infrastructures.

Governance by the Industries

Today, information and network assets are as important as financial assets for companies. Enterprises depend on their network to reach and support customers and suppliers. When a network fails to perform, costs will increase, reputations will suffer and transactions will be lost. Privacy and integrity losses may create liabilities and create costs. Maintaining a continuous business in a global, networked society is critical.

In the wake of the attacks of September 11 and CEOs' responsibility for matters of corporate management, it is increasingly important for senior management to ensure that their networks can support business continuity and profitability objectives.

A trend appears to have developed toward a new form of accountability and responsibility for owners and operators of enterprise networks. In such an environment, enterprises may choose to appoint a Chief Information Security Officer (CISO) or adopt alternative measures to ensure security. Not only CEOs but also senior management should be accountable for, and recognize security management, as indispensable for corporate management.

Enterprises should develop business processes for security management and establish a security management system, operated and initiated by senior management.

The following items should be indispensable for global corporations and their leaders.

- A Security Policy, which clearly states the position and basic understanding of the corporation regarding information security, for example, how to protect information and data inside its own information network and system, should be established. Security Program including business continuity in emergency situation would be also effective.

- A CISO, who is responsible for information security at board level, may be appointed. He/She should be responsible for ensuring policy consistency, clearly defining policies, identifying and consistently enforcing consequences for non-compliance, and instituting a governance framework to monitor and control the execution of processes and procedures.

- Security management systems and programs should be established and operated effectively. They should be based on risk assessment and should be dynamic, encompassing all levels of corporate activity and all aspects of corporate operations, and be initiated under the leadership of the CEO. Information system and network security policies, practices, measures and procedures should be co-oriented and integrated by security management to create a coherent system of security.

- Systems, networks and policies of corporations need to be properly designed, implemented and coordinated to optimize cyber security. Cyber security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. Corporations should respect and implement this principle not only as a provider of services and devices for information systems but also as an owner or operator of its own information systems and network.

Internet Protection

In recent years, the number of information systems damaged by hackers, viruses, and other cyber attacks has increased dramatically. To avoid and prevent damage, one possible solution for governments is to enact new laws or amend existing laws to be harmonized with the participating countries.

However, law enforcement can be burdensome for industries and impact on business development. Rather than place the burden on infrastructure corporations and ISPs to store and preserve great amounts of data and provide access to law enforcement, focusing on new or revised legislation enabling more effective education, awareness, and deterrence would be a better approach.

Best Practice

Best practices are intended as voluntary guidelines to be considered by a company when deciding on a commercial activity and thereby increasing information security.

Issues to be taken into consideration in drafting the best practices:

a. *Sustainability*: the viability over time of a commercial activity, including the prospect of a long-term return internally generated by the activity;

b. *Appropriate technology*: the choice of an ICT technology adapted for the market within a developing country that is suitable within geographic and environment constraints, targeted for skill-sets and objectives of users, to ensure take-up of the technology and commercial return;

c. *Local contents*: software or other contents, developed in the target country or region, to be included in the product or service offered, both as a tool to meet local market characteristics and also to bring local partners into its development.

Other best practices are also important:

a. *Scalability*: the ability easily to increase the scope, geographic reach or target audience of an investment or other commercial activity, at the time, for example, the concept underlying the activity has been demonstrated;

b. *Local partners*: the involvement of corporations and industries from the developing country or region for, among other reasons, their skill at development of content or other input, knowledge of the target market, marketing, sharing of commercial (and regulatory) risk and reward especially with regards to the issue of Information sharing.

Recommendations for public authorities

Public authorities in developing countries are encouraged to adopt laws reducing barriers to investment, ensuring a stable commercial environment, and meeting international treaty obligations.

Public authorities should be aware of the business decision process undertaken and the criteria applied by a company when deciding on a commercial activity in a developing country.

Public authorities should also be aware that a commercial activity can achieve not only a commercial return for the company but also meet development objectives. In many cases, a commercial activity is the best method to achieve economic development and alleviation of poverty.

At the same time, the Public Authorities should play the part of Law Enforcement with regards to Imposing the Obligations on the industries and thereby reporting to the Government and Treaties to suggest remedial issues to upgrade the system further.

Recommendations for industry

- A company is encouraged to use these best practices when considering whether to make, in a developing country an investment or to undertake other commercial activities in information and communications technology.
- Companies are encouraged to exchange information (among themselves and with other stakeholders) on their commercial activities addressing the digital divide in emerging economies, to develop together further the best practices they use for assessing such activities, and to measure the commercial and other

Reason for the Need of a Uniformed Law

In the event that there is no Uniformed law, it would create Legal Problems and Practical Difficulties. Mechanism must be based on peaceful coo-existence principles and no country should seek regional hegemony.

Although the Cold War ended some years ago and the East and West are getting closer to each other, the differences between them still exist when it comes to treaties for cooperation in criminal justice.

China has legal assistance treaties with important western countries such as France, Belgium, Italy and Spain, but in civil and commercial matters only. Countries that are parties to extradition and criminal mutual legal assistance treaties with China are mostly from the former socialist bloc.

Reason for the Need of a Uniformed Law

China appears to give priority to the region stability in order to continue with the momentum of its economic and social developments.

As in many existing treaties, the United Nations Model Treaties on extradition and mutual legal assistance provides a number of restrictions that are either grounds for refusal or factors for consideration of approvals.

To build up a new security mechanism in the Asia-Pacific region, it is necessary to seek consensus on mutual trust. It is the most important prerequisite for regional security building and arrangements.

The Potential Problems

- ***Double criminality.***

- ***Extradition Issues.***
- ***Prejudice against the offender.***
- ***Risk to public order.***
- ***Lack of procedural guarantees.***
- ***Judicial independence and fair trial.***
- ***Punishment and treatment of offenders.***
- ***Insufficient proof.***

Confidentiality and Non-Disclosure

All the information contained in this proposal shall be treated private and confidential. The party receiving it shall not disclose it to other party not related to the business objective intended by this document.

Ownership of the Copyright